

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO BÀI TẬP CÁ NHÂN
HỌC PHẦN: MẬT MÃ HỌC CƠ SỞ
MÃ HỌC PHẦN: INT1344

ĐỀ TÀI: TÌM HIỂU VỀ VPN

Sinh viên thực hiện:

Đinh Thị Thanh Tâm

B22DCAT253

Giảng viên hướng dẫn: Quản Trọng Thế

Tên lớp: 01

HÀ NỘI 3-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ	5
DANH MỤC CÁC BẢNG BIỂU	7
DANH MỤC CÁC TỪ VIẾT TẮT	8
Layer 2 Tunneling Protocol	8
LỜI MỞ ĐẦU	10
CHƯƠNG 1. Tổng quan về VPN	11
1.1 Khái niệm.....	11
1.2 Chức năng	13
1.3 Thành phần chính của VPN.....	14
1.4 Các mode kết nối VPN.	14
1.4.1 Tunnel Mode	15
1.4.2 Transport mode	16
1.5 Cách thức hoạt động	16
1.6 Công dụng của VPN	17
1.6.1 Bảo mật tuyệt đối khi kết nối Wifi công cộng	17
1.6.2 Bảo mật dữ liệu khỏi những ứng dụng và dịch vụ.....	18
1.6.3 Bảo mật dữ liệu khỏi nhà cung cấp mạng	18
1.6.4 Truy cập trang web mọi lúc mọi nơi	18
1.6.5 Download ẩn danh.....	19
1.7 Ưu điểm và nhược điểm của VPN.....	19
1.7.1 Ưu điểm.....	19
1.7.2 Nhược điểm:.....	19
1.8 Cách thiết lập mạng VPN	20
1.8.1 Sử dụng nhà cung cấp dịch vụ VPN	20
1.8.2 Sử dụng bộ định tuyến VPN	20
1.8.3 Hướng dẫn cài đặt và sử dụng VPN đơn giản.....	21
1.9 Kết chương.....	22
CHƯƠNG 2. Cấu trúc và giao thức trong VPN	23
2.1 Cấu trúc và cách thức hoạt động.....	23

2.1.1 VPN Server	23
2.1.2 VPN Client	23
2.1.3 VPN Tunnel.....	23
2.2 Phân loại VPN	24
2.2.1 VPN truy cập từ xa(Remote Access VPN)	24
2.2.2 Mạng VPN cục bộ (Intranet-based VPN)	26
2.2.3 2. Mạng VPN mở rộng (Extranet-based VPN)	27
2.2.4 VPN truy cập từ xa so với VPN Site-to-Site.....	29
2.3 Các giao thức đường hầm phổ biến	29
2.3.1 Giao thức chuyển tiếp lớp 2 (L2F – Layer Two Forwarding)	29
2.3.2 Giao thức đường hầm điểm tới điểm (PPTP - Point-To-Point Tunneling Protocol)	31
2.3.3 Giao thức bảo mật IP (IPSec – Internet Protocol Security)	32
2.3.4 Mạng riêng ảo trên nền MPLS	40
2.3.5 So sánh MPLS-VPN với IPSec-VPN	43
2.3.6 Ngoài ra, còn một số giao thức phổ biến khác.....	44
2.3.7 Cách chọn giao thức phù hợp.....	45
2.4 Kết chương.....	45
CHƯƠNG 3. : CÁC VẤN ĐỀ AN NINH CỦA VPN.....	46
3.1 Hệ thống phát hiện xâm nhập dựa trên khai phá dữ liệu trong VPN	46
3.1.1 Giới thiệu.....	46
3.1.2 Tổng quan về hệ thống phát hiện xâm nhập (IDS)	46
3.1.3 Cấu trúc hệ thống IDS	47
3.1.4 Hệ thống phát hiện xâm nhập dựa trên khai phá dữ liệu	47
3.1.5 Hệ thống phát hiện xâm nhập trong ứng dụng VPN.....	48
3.2 Mạng VPN liên nhà cung cấp sử dụng phương pháp VRF Back-to-Back và MP-eBGP	49
3.2.1 Giới thiệu.....	49
3.2.2 Mạng riêng ảo VPN.....	49
3.2.3 Công nghệ MPLS và VPN	51
3.2.4 Thách thức của VPN Internet.....	51

3.2.5 Mạng VPN liên nhà cung cấp (Inter-Provider VPN).....	52
3.2.6 Kết quả mô phỏng	53
3.3 Phân tích VPN và Góc nhìn Mới để Bảo vệ Mạng Thoại qua VPN	54
3.3.1 Giới thiệu.....	54
3.3.2 Giao thức VPN (VPN Protocols)	55
3.3.3 Bảo mật thoại trên VPN (Voice over VPN Security)	57
3.3.4 Giải pháp bảo mật đề xuất (Proposed Security Solution).....	58
3.4 Khắc phục các lỗ hổng bảo mật trong triển khai mạng không dây dựa trên VPN.....	61
3.4.1 Giới thiệu.....	61
3.4.2 Bộ định tuyến không dây ẩn (Hidden Wireless Router – HWR).....	63
3.4.3 Phát hiện và phòng chống lỗ hổng HWR.....	64
3.5 Kết chương.....	71
CHƯƠNG 4. DEMO sử dụng Giải pháp dựa trên giám sát (Monitoring-Based Solutions) để phát hiện lỗ hổng HWR	72
4.1 Chuẩn bị mô hình mạng.....	72
4.2 CẤU HÌNH CHUNG CHO CÁC MÁY ẢO.....	73
4.2.1 Máy H (Windows 10 - HWR).....	73
4.2.2 Máy R (Kali Linux - Attacker).....	74
4.2.3 Máy S (Kali Linux - Sniffer).....	74
4.2.4 Máy VPN Server (Windows Server).....	75
4.2.5 Kiểm tra cấu hình	75
4.3 CÁC BƯỚC THỰC HIỆN	77
4.3.1 Trên máy Sniffer	77
4.3.2 Từ máy R (Kali – Rogue), thực hiện gửi gói không qua VPN	77
4.3.3 Quan sát từ Sniffer	78
4.3.4 Kết quả phân tích gói tin:	79
4.3.5 Có thể lọc chi tiết hơn	79
4.4 Kết chương.....	80
KẾT LUẬN	81
TÀI LIỆU THAM KHẢO.....	82

DANH MỤC CÁC HÌNH VẼ

Hình 1 Khi sử dụng và Không sử dụng VPN	11
Hình 2 VPN giúp cho việc kết nối an toàn hơn	12
Hình 3 Mô hình kết nối VPN từ mạng gia đình đến mạng văn phòng	13
Hình 4 Các thành phần của VPN	14
Hình 5 Hai chế độ kết nối VPN để chuyển dữ liệu giữa hai thiết bị	15
Hình 6 Mô hình bảo vệ dữ liệu thông qua VPN	16
Hình 7 So sánh mức độ an toàn khi kết nối Wi-Fi công cộng với và không có VPN	18
Hình 8 Thiết bị phát sóng Wi-Fi (Router) trong mạng nội bộ.....	21
Hình 9 Hướng dẫn cài đặt và sử dụng VPN đơn giản.....	21
Hình 10 Hướng dẫn cài đặt và sử dụng VPN đơn giản	22
Hình 11 Mô hình VPN đơn giản	23
Hình 12 Mô hình VPN truy cập từ xa(Remote Access VPN)	24
Hình 13 Mô hình VPN Site-to-Site (Intranet Based).....	27
Hình 14 Mô hình VPN Site-to-Site (Extranet-Based VPN)	28
Hình 15 Cấu trúc gói của giao thức L2F.....	29
Hình 16 Mô hình hệ thống của giao thức L2F.....	30
Hình 17 Hệ thống cung cấp VPN dựa trên PPTP	31
Hình 18 Cấu trúc gói PPTP.....	32
Hình 19 Sơ đồ đóng gói PPTP	32
Hình 20 Mô hình sử dụng VPN trên nền IPSec.....	32
Hình 21 Cấu trúc tiêu đề ESP	33
Hình 22 Giao thức đóng gói tải tin an toàn ESP	33
Hình 23 Khuôn dạng gói tin Ipv4 trước và sau khi xử lý ESP	33
Hình 24 Khuôn dạng gói tin Ipv6 trước và sau khi xử lý ESP	34
Hình 25 Cấu trúc tiêu đề AH.....	34
Hình 26 Khuôn dạng gói tin Ipv4 trước và sau khi xử lý AH	35
Hình 27 Khuôn dạng gói tin Ipv6 trước và sau khi xử lý AH	35
Hình 28 Xử lý gói tin IP ở chế độ truyền tải.....	36
Hình 29 Xử lý gói tin IP ở chế độ đường hầm.....	36
Hình 30 Kết hợp SA kiểu đường hầm khi hai hay một điểm cuối trùng nhau ...	37
Hình 31 Đường hầm IPSec được thiết lập	37
Hình 32 Kiến trúc của IPSec	39
Hình 33 Hệ thống cung cấp VPN dựa trên L2TP	39
Hình 34 Cấu trúc gói dữ liệu L2TP.....	40
Hình 35 Hoạt động chuyển tiếp dữ liệu VPN qua mạng MPLS.....	40

Hình 36 Các thành phần cơ bản của MPLS-VPN.....	41
Hình 37 Bộ định tuyến PE và sơ đồ kết nối các site khách hàng	42
Hình 38 Sử dụng nhãn để chuyển tiếp gói tin VPN.....	42
Hình 39 Sử dụng ngăn xếp nhãn để chuyển tiếp gói tin VPN	42
Hình 40 Sơ đồ mô tả chức năng của hệ thống phát hiện xâm nhập.....	47
Hình 41 Hệ thống phát hiện xâm nhập trong ứng dụng VPN.....	49
Hình 42 Mô hình MPLS L3VPN	50
Hình 43 Mô hình MPLS L2VPN	50
Hình 44 Mô hình kiến trúc bảo mật thoại qua VPN: Người dùng Alice và Bob kết nối qua đường hầm VPN bảo mật. Cuộc gọi thoại định tuyến qua các SIP Proxy và truyền qua Internet nhưng vẫn giữ được tính riêng tư nhờ cơ chế mã hóa VPN.	59
Hình 45 Chiến lược triển khai mạng không dây hiện tại	62
Hình 46 Mô tả chi tiết tình huống tấn công	64
Hình 47 Cấu hình mạng máy ảo.....	72
Hình 48 Cấu hình 2 NIC máy H	73
Hình 49 Cấu hình IP máy H.....	74
Hình 50 Cấu hình IP máy r	74
Hình 51 Cấu hình IP máy S.....	75
Hình 52 Cấu hình IP máy VPN Server	75
Hình 53 Từ máy H ping đến máy VPN Server	75
Hình 54 Từ máy H ping đến máy R.....	76
Hình 55 Từ máy H ping đến máy Sniffer	76
Hình 56 Từ máy R ping đến máy H.....	76
Hình 57 Từ máy R ping đến máy Sniffer.....	76
Hình 58 Từ máy Sniffer ping đến máy H	77
Hình 59 Từ máy Sniffer ping đến máy R.....	77
Hình 60 Lệnh bắt toàn bộ gói.....	77
Hình 61 Ping từ máy R đến máy VPN Server	78
Hình 62 Máy R truy cập địa chỉ máy VPN Server	78
Hình 63 Quan sát từ máy Sniffer	79
Hình 64 Lọc theo IP nguồn	80
Hình 65 Lọc ICMP (ping).....	80

DANH MỤC CÁC BẢNG BIỂU

Bảng 1. Bảng so sánh MPLS-VPN với IPSec-VPN	44
Bảng 2. Bảng so sánh các giao thức VPN.....	57
Bảng 3. Bảng so sánh ưu điểm với VPN truyền thống	60
Bảng 4. Bảng cấu hình thành phần các máy ảo	73

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
VPN	Virtual Private Network	Mạng riêng ảo
PPTP	Point-to-Point Tunneling Protocol	Giao thức đường hầm điểm-điểm
SSTP	Secure Socket Tunneling Protocol	Giao thức đường hầm ổ cắm bảo mật
L2TP	Layer 2 Tunneling Protocol	Giao thức đường hầm tầng 2
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa nâng cao
QoS	Quality of Service	Chất lượng dịch vụ
SSL	Secure Sockets Layer	Lớp ổ cắm bảo mật
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình máy chủ động
DNS	Domain Name Servers	Máy chủ tên miền
ADSL	Asymmetric Digital Subscriber Line	Đường dây thuê bao số bất đối xứng
ISP	Internet Service Provider	Nhà cung cấp dịch vụ Internet
LAN	Local Area Network	Mạng cục bộ
NAT	Network Address Translation	Biên dịch địa chỉ mạng
CPU	Central Processing Unit	Bộ xử lý trung tâm
PE	Provider Edge	Thiết bị biên cung cấp dịch vụ
TLS	Transport Layer Security	Giao thức giao tiếp bảo mật
ASBR	Autonomous System Boundary Router	Bộ định tuyến biên hệ thống tự trị
VRF	Virtual Routing and Forwarding instance	Định tuyến và chuyển tiếp ảo
RD	Route Distinguisher	Bộ phân biệt tuyến đường

MP-BGP	Multiprotocol BGP	Phần mở rộng Multiprotocol dành cho BGP
RR	Route Reflector	Bộ phản chiếu tuyến
OSPF	Open Shortest Path First	
EIGRP	Enhanced Interior Gateway Routing Protocol	
eBGP	External Border Gateway Protocol	
RT	Route Target	
LER	Label Edge Routers	Router ở biên
LSR	Label Switch Routers	
LDP	Label Distribution Protocol	Giao thức phân phối nhãn
RSVP-TE	Resource Reservation Protocol - Traffic Engineering	Giao thức Dự trữ Tài nguyên - Kỹ thuật Lưu lượng
OTP	One Time Password	Mật khẩu một lần
VPNaaS	VPN-as-a-Service	
JWT	JSON Web Tokens	Mã thông báo Web JSON

LỜI MỞ ĐẦU

Trong bối cảnh công nghệ thông tin phát triển mạnh mẽ và nhu cầu trao đổi dữ liệu từ xa ngày càng cao, vấn đề bảo mật thông tin khi truyền qua mạng Internet trở thành một trong những mối quan tâm hàng đầu của cá nhân, tổ chức và doanh nghiệp. Môi trường mạng công cộng luôn tiềm ẩn nhiều rủi ro bảo mật như nghe lén, đánh cắp dữ liệu, giả mạo truy cập... Trong hoàn cảnh đó, công nghệ mạng riêng ảo – **VPN (Virtual Private Network)** – đã ra đời và trở thành giải pháp hữu hiệu giúp bảo vệ tính riêng tư, toàn vẹn và an toàn cho luồng dữ liệu giữa các điểm kết nối.

VPN không chỉ đơn thuần là một lớp bảo vệ cho người dùng cá nhân mà còn là thành phần không thể thiếu trong hệ thống mạng doanh nghiệp, đặc biệt là trong các mô hình làm việc từ xa, kết nối đa chi nhánh, truy cập nội bộ từ bên ngoài. Nắm vững cấu trúc, giao thức, cách thức hoạt động và các mối đe dọa an ninh liên quan đến VPN là điều cần thiết đối với sinh viên ngành công nghệ thông tin cũng như các kỹ sư hệ thống.

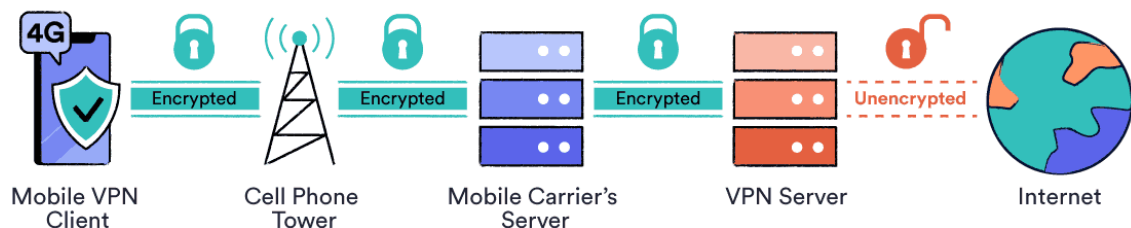
Báo cáo này được thực hiện với mục tiêu tổng hợp kiến thức cơ bản và nâng cao về VPN, phân tích các vấn đề bảo mật phổ biến, đồng thời tiến hành mô phỏng thực nghiệm tấn công mạng nhằm phát hiện các lỗ hổng trong triển khai VPN. Thông qua đó, người học không chỉ tiếp cận kiến thức lý thuyết mà còn phát triển kỹ năng đánh giá, kiểm thử và áp dụng giải pháp bảo vệ hệ thống mạng thực tế một cách hiệu quả.

CHƯƠNG 1. TỔNG QUAN VỀ VPN

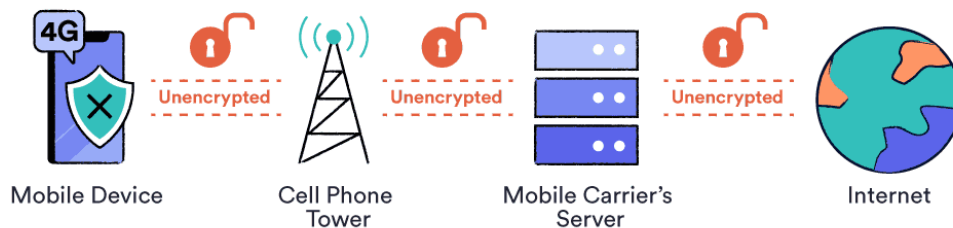
1.1 Khái niệm

Mạng riêng ảo (VPN), viết tắt của Virtual Private Network, là một công nghệ cho phép mở rộng mạng riêng qua mạng công cộng như internet, tạo ra kết nối an toàn và mã hóa. Mục tiêu chính của VPN là bảo vệ quyền riêng tư trực tuyến, che giấu địa chỉ IP của người dùng và mã hóa dữ liệu để ngăn chặn các bên thứ ba như nhà cung cấp dịch vụ internet (ISP), hacker, hoặc chính phủ theo dõi hoặc đánh cắp thông tin. VPN tạo ra một "đường hầm" mã hóa, làm cho dữ liệu trở nên vô nghĩa với bất kỳ ai không có khóa giải mã, đặc biệt hữu ích khi sử dụng Wi-Fi công cộng ở quán cà phê, sân bay, hoặc khách sạn.

With A VPN



Without A VPN

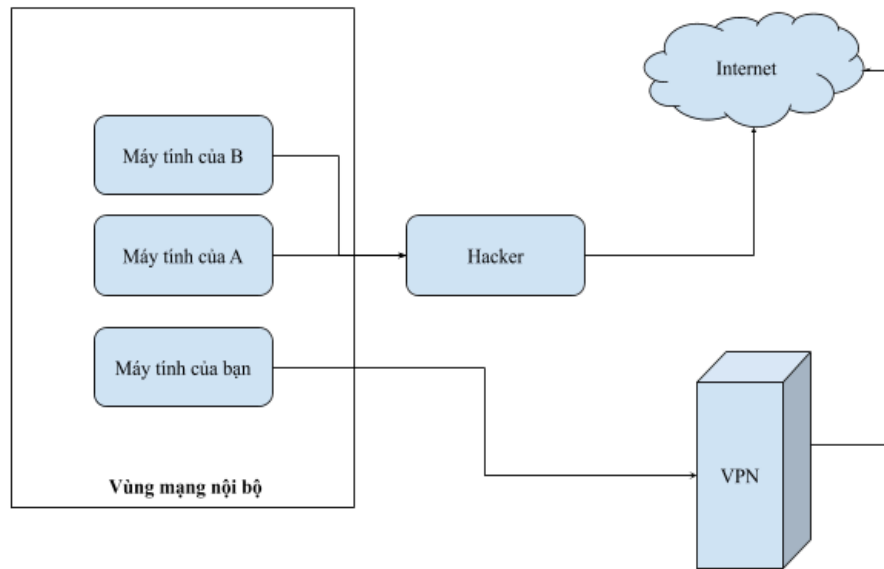


Hình 1 Khi sử dụng và Không sử dụng VPN

Dưới đây là những lý do mà VPN được hình thành:

- Ví dụ năm 2010, tại Việt Nam chúng ta không thể truy cập được đến Facebook. Lúc này việc sử dụng VPN sẽ giúp chúng ta có thể “qua mặt” và kết nối với Facebook bình thường.
- Hoặc khi chúng ta sử dụng các mạng Internet công cộng như tại quán cafe hay các địa điểm Internet miễn phí, lúc này sẽ có nhiều người cùng kết nối chung vào một mạng. Và đây là cơ hội tốt cho các cuộc tấn công mạng. Hacker, bằng một thủ thuật nào đó sẽ có thể chặn và bắt được các thông tin bạn gửi lên Internet. Lúc này với VPN nó sẽ tạo ra một vùng mạng riêng. Nó vẫn giúp bạn

kết nối Internet như bình thường, đồng thời người khác cũng khó có thể đánh cắp thông tin của bạn hơn.

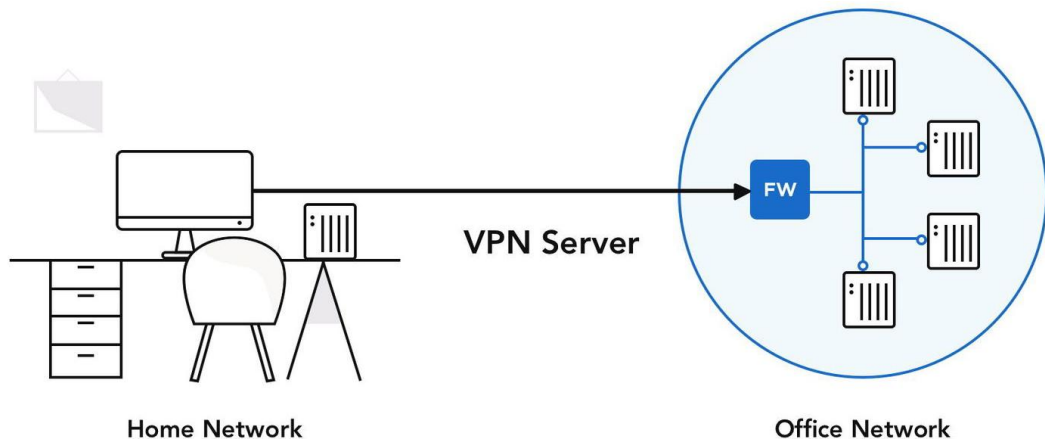


Hình 2 VPN giúp cho việc kết nối an toàn hơn

Giả sử Việt là một nhân viên làm việc từ xa cho một công ty có trụ sở chính tại Hồ Chí Minh, Việt sống ở một thành phố khác và thường làm việc từ nhà. Để thực hiện công việc hàng ngày, Việt cần truy cập vào các tài nguyên nội bộ của công ty như các tập tin quan trọng, cơ sở dữ liệu, source code và các ứng dụng doanh nghiệp chỉ có sẵn trên mạng nội bộ của công ty.

Việt cần cài đặt một phần mềm VPN client trên máy tính của mình. Công ty của anh đã cung cấp thông tin đăng nhập và các hướng dẫn cần thiết để thiết lập kết nối VPN. Khi bắt đầu ngày làm việc, Việt mở ứng dụng VPN client và nhập tên người dùng và mật khẩu của mình. VPN client sau đó sẽ tạo một kết nối an toàn tới máy chủ VPN của công ty đặt tại trụ sở chính ở Hồ Chí Minh.

Máy chủ VPN xác thực thông tin của Việt và sử dụng các giao thức bảo mật như IPsec hoặc SSL để thiết lập một "đường hầm" (tunnel) mã hóa giữa máy tính của Việt và mạng nội bộ của công ty. Dữ liệu truyền qua đường hầm này được mã hóa, giúp bảo vệ khỏi việc bị chặn hoặc truy cập trái phép.



Hình 3 Mô hình kết nối VPN từ mạng gia đình đến mạng văn phòng

Sau khi kết nối VPN được thiết lập, Việt có thể truy cập các tài nguyên nội bộ của công ty như thể anh đang làm việc tại văn phòng. Anh có thể mở các tệp tin từ máy chủ công ty, truy cập cơ sở dữ liệu, và sử dụng các ứng dụng nội bộ để thực hiện công việc của mình.

Nhờ VPN, tất cả dữ liệu Việt gửi và nhận đều được mã hóa, đảm bảo rằng thông tin nhạy cảm của công ty không bị rò rỉ hoặc bị truy cập trái phép. Điều này đặc biệt quan trọng khi Việt làm việc từ các mạng công cộng như Wi-Fi tại quán cà phê.

1.2 Chức năng

VPN cung cấp 3 chức năng chính:

- **Tính tin cậy (Confidentiality):** là khả năng giữ cho dữ liệu được an toàn và bảo mật trong quá trình truyền qua mạng. VPN đảm bảo điều này bằng cách mã hóa các gói dữ liệu trước khi gửi đi. Nhờ đó, ngay cả khi có ai đó chặn được các gói dữ liệu trong quá trình truyền tải, họ cũng không thể đọc được nội dung bên trong. Việc mã hóa giúp ngăn chặn truy cập trái phép và bảo vệ thông tin nhạy cảm khỏi bị rò rỉ.
- **Tính toàn vẹn (Data Integrity)** dữ liệu đảm bảo rằng dữ liệu không bị thay đổi hoặc giả mạo trong quá trình truyền từ người gửi đến người nhận. Khi sử dụng VPN, người nhận có thể kiểm tra tính toàn vẹn của dữ liệu thông qua các thuật toán kiểm tra như hàm băm (hash function). Điều này giúp phát hiện nếu có bất kỳ sự thay đổi nào xảy ra trên đường truyền, từ đó loại bỏ các gói dữ liệu bị sửa đổi và bảo vệ độ chính xác của thông tin.
- **Tính xác thực (Origin Authentication)** liên quan đến việc xác minh danh tính của người gửi dữ liệu. VPN sử dụng các cơ chế xác thực như chứng thực bằng

mật khẩu, khóa mã hóa, hoặc chứng chỉ số để đảm bảo rằng dữ liệu được gửi từ đúng nguồn hợp lệ. Điều này giúp người nhận có thể tin tưởng vào nguồn gốc của thông tin, đồng thời ngăn chặn các cuộc tấn công giả mạo hoặc truy cập trái phép vào hệ thống.

1.3 Thành phần chính của VPN



Hình 4 Các thành phần của VPN

VPN bao gồm các thành phần cơ bản sau:

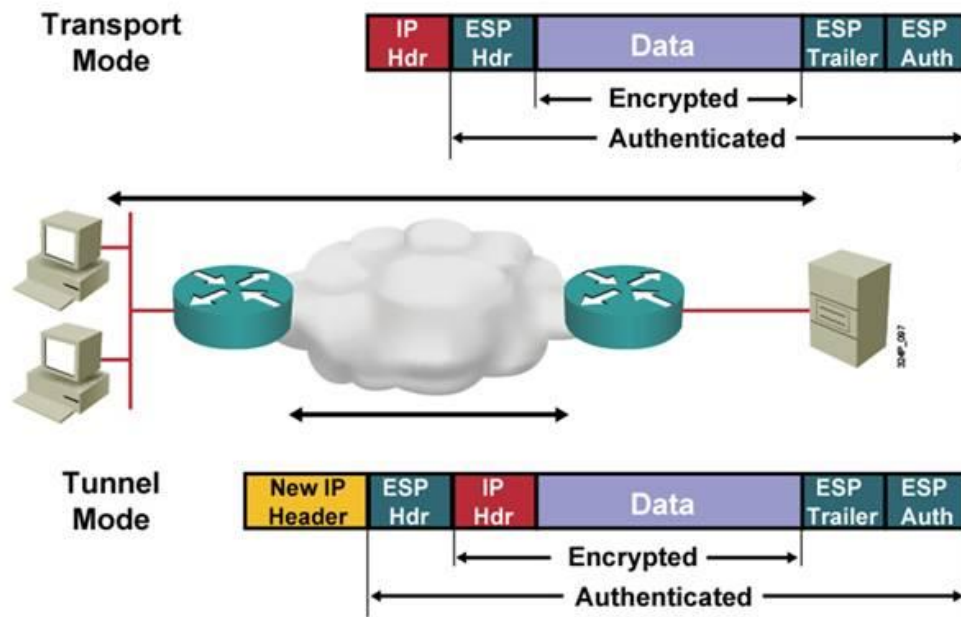
- Thiết bị người dùng (Client): Đây là thiết bị của người dùng, như máy tính, điện thoại thông minh, hoặc máy tính bảng, kết nối với mạng VPN.
- Máy chủ VPN (VPN Server): Máy chủ do nhà cung cấp VPN vận hành, đóng vai trò trung gian xử lý và chuyển tiếp dữ liệu. Máy chủ này có thể nằm ở nhiều quốc gia, giúp người dùng thay đổi địa điểm ảo.
- Mã hóa: Dữ liệu được mã hóa để bảo vệ trong quá trình truyền tải. Phương pháp mã hóa phổ biến là AES-256, được coi là một trong những tiêu chuẩn mã hóa mạnh nhất hiện nay.
- Giao thức: Các giao thức VPN quyết định cách dữ liệu được mã hóa và truyền tải.

1.4 Các mode kết nối VPN.

Có hai chế độ kết nối VPN để chuyển dữ liệu giữa hai thiết bị:

- Tunnel mode
- Transport mode

Cả hai mode này định nghĩa quá trình đóng gói được sử dụng để di chuyển dữ liệu một cách an toàn giữa hai thực thể.



Hình 5 Hai chế độ kết nối VPN để chuyển dữ liệu giữa hai thiết bị

1.4.1 Tunnel Mode

Một hạn chế của transport mode là không có khả năng mở rộng. Do đó, nếu chúng ta có nhiều thiết bị ở hai vị trí riêng biệt cần nói nhiều chuyện với nhau trong chế độ bảo mật, mình khuyên các bạn nên sử dụng tunnel mode thay vì transport mode.

Trong tunnel mode, các thiết bị nguồn-đích thực thông thường sẽ không bảo vệ dữ liệu, thay vào đó các thiết bị trung gian được sử dụng để bảo vệ luồng dữ liệu. Các thiết bị này được gọi là các VPN gateway.

Tunnel mode cung cấp nhiều tính năng ưu việt hơn Transport mode:

- Tính mở rộng: ta có thể chọn một thiết bị phù hợp để thực hiện việc xử lý bảo vệ.
- Tính linh động: không cần phải thay đổi gì trong cấu hình VPN khi thêm vào một thiết bị mới sau VPN Gateway.
- Tính ẩn của các giao tiếp: các lưu lượng được các VPN Gateway đại diện trao đổi với nhau, vì vậy sẽ che dấu nguồn và đích thật sự của kết nối.
- Sử dụng địa chỉ cục bộ: các thiết bị đích và nguồn thực có thể sử dụng địa chỉ được đăng kí (public) hay cục bộ bởi vì các gói tin được sử dụng bởi các VPN Gateway.

- Sử dụng các chính sách bảo mật hiện có: các chính sách bảo mật được thực hiện trên các thiết bị tường lửa và bộ lọc gói tin.

1.4.2 Transport mode

Một kết nối ở mode transport được sử dụng địa chỉ IP nguồn và đích thật sự của các thiết bị trong các gói tin để truyền dữ liệu.

1.5 Cách thức hoạt động

Chúng ta sử dụng Internet hàng ngày để lướt web, dùng Facebook hay xem phim,... Cho dù chúng ta làm gì đi chăng nữa thì nó đều trải qua các bước như sau:

- Bước 1: Khi bạn thao tác với mạng Internet bằng các hành động trên, ngay lập tức dữ liệu sẽ bắt đầu xuất phát từ máy tính hoặc các thiết bị cầm tay của bạn để ra ngoài. Giả sử bạn truy cập vào website của Viettel IDC tại địa chỉ <https://viettelidc.com.vn/>. Lúc này hệ thống sẽ phân giải tên miền thành địa chỉ IP và tìm kiếm nó trên Internet. Lúc này Web server khi nhận được yêu cầu truy cập của bạn nó sẽ tìm kiếm dữ liệu và trả về các thông tin mà bạn cần. Và đây là chu trình đi.
- Bước 2: Nhưng có một vấn đề là làm thế nào để Web server biết được người dùng nào vừa mới gửi yêu cầu truy cập đến Viettel IDC mà trả về thông tin cho họ? Khi người dùng gửi thông tin đến Web server thì đính kèm với đó là địa chỉ IP máy của họ. Và như vậy lúc này Web server sẽ hiểu được ai là người vừa gửi yêu cầu cho họ để trả lại thông tin cho chính xác. Lúc này, khi đã có được địa chỉ IP của người dùng và yêu cầu truy cập của họ rồi thì Web server sẽ gửi lại những thông tin theo yêu cầu đó của họ. Và đây là chu trình về.



Hình 6 Mô hình bảo vệ dữ liệu thông qua VPN

VPN hoạt động bằng cách tạo ra một "đường hầm" an toàn giữa hai hoặc nhiều thiết bị. Bên trong đường hầm này, dữ liệu được mã hóa nhằm ngăn chặn truy cập trái phép. Sau đây là các bước của quá trình tạo kết nối VPN:

- Yêu cầu kết nối: Người dùng khởi tạo kết nối tới máy chủ VPN, thường bằng cách khởi động phần mềm VPN client.
- Xác thực: Máy chủ xác minh thông tin đăng nhập của người dùng (username/password, key). Nếu thông tin được xác minh, một kết nối an toàn sẽ được thiết lập.
- Thiết lập kết nối an toàn: Khi đã được xác thực, một đường hầm an toàn được hình thành giữa thiết bị của người dùng và máy chủ VPN. Đường hầm này hoạt động như một lối đi được bảo vệ.
- Đóng gói (Encapsulation): Dữ liệu của người dùng được bọc trong một giao thức VPN, tạo ra một "vỏ ngoài" bảo vệ nội dung bên trong.
- Mã hóa (Encryption): Dữ liệu truyền qua kết nối được mã hóa bằng các thuật toán như AES (Advanced Encryption Standard).
- Truyền tải: Dữ liệu đã mã hóa được gửi qua mạng công cộng đến máy chủ VPN.
- Giải đóng gói và giải mã (Decapsulation and Decryption): Khi đến máy chủ VPN, vỏ ngoài được loại bỏ (giải đóng gói) và dữ liệu được giải mã.
- Truyền tải lần cuối: Dữ liệu gốc được gửi an toàn từ máy chủ VPN đến địa chỉ đích.

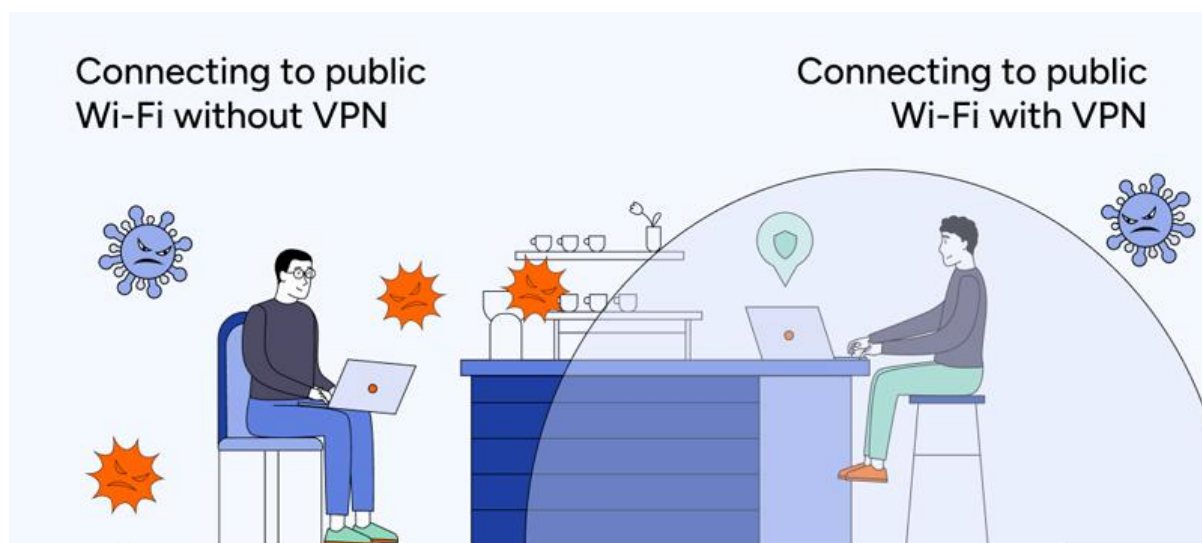
Toàn bộ quá trình trên đảm bảo rằng dữ liệu vẫn giữ được tính riêng tư và an toàn khi di chuyển từ điểm này đến điểm khác.

1.6 Công dụng của VPN

1.6.1 Bảo mật tuyệt đối khi kết nối Wifi công cộng

Công nghệ thông tin phát triển mạnh mẽ, nhu cầu kết nối Wifi của người dùng tăng lên, bạn dễ thấy Wifi Free có thể xuất hiện ở mọi nơi. Wifi Free là một con dao hai lưỡi với người dùng. Khi bạn phản hồi email công việc tại tiệm bánh hay vô thức lướt đa phương tiện tại nhà hàng, rất có thể mọi hoạt động trực tuyến của bạn đang bị ai đó theo dõi.

Lúc này, VPN sẽ phát huy vai trò của mình, bảo vệ mọi dữ liệu khi bạn truy cập những kết nối mạng bên ngoài, ẩn trình duyệt, các thông tin cá nhân cũng như một số mật khẩu quan trọng tránh bị tin tặc xâm hại.



Hình 7 So sánh mức độ an toàn khi kết nối Wi-Fi công cộng với và không có VPN

1.6.2 Bảo mật dữ liệu khỏi những ứng dụng và dịch vụ

Một số ứng dụng và dịch vụ Internet hiện nay rất đáng quan ngại, điển hình như Facebook, Youtube hay Shopee,...những ứng dụng này có thể thu thập và sử dụng dữ liệu của người dùng. VPN có công dụng ngăn chặn những ứng dụng này theo dõi, thu thập vị trí, dữ liệu truy cập và hành vi sử dụng của bạn trên các ứng dụng đó.

1.6.3 Bảo mật dữ liệu khỏi nhà cung cấp mạng

Kết nối Wifi tại nhà sẽ hạn chế tối đa khả năng bị xâm nhập và đánh cắp dữ liệu. Tuy nhiên, một mối lo ngại khác là ISP, nhà cung cấp mạng có thể truy cập hệ thống dữ liệu để định vị bạn ở đâu, đang làm gì và sử dụng mạng của họ như thế nào.

Những dữ liệu này có thể được thu thập và bán ra cho những nhà tiếp thị/quảng cáo ngay cả khi trang web của bạn đã được kích hoạt chức năng bảo mật. VPN sẽ là nhân tố quan trọng bảo vệ địa chỉ IP của bạn khỏi ISP bằng cách ẩn định vị.

1.6.4 Truy cập trang web mọi lúc mọi nơi

Với tính năng ẩn định vị, bạn có thể kết nối với các máy chủ ở bất kỳ nơi nào. Nhờ vậy mà bạn có thể truy cập mọi trang web, nội dung từ quốc tế và không bị giới hạn về quốc gia.

Bên cạnh đó, tính năng mã hoá của VPN cũng rất hữu ích, giúp bảo vệ thông tin một cách an toàn và hiệu quả.

1.6.5 Download ẩn danh

Download phần mềm/ứng dụng là nhu cầu thiết yếu của người dùng. Tuy nhiên, quá trình này gặp nhiều hạn chế liên quan đến các phần mềm độc hại, mã độc, virus. VPN có công dụng như một tấm khiên chắn, bảo vệ người dùng download an toàn.

1.7 Ưu điểm và nhược điểm của VPN

1.7.1 Ưu điểm

- Bảo mật: VPN mã hóa lưu lượng truy cập internet của bạn, giúp bảo vệ dữ liệu khỏi những kẻ xâm nhập và tin tặc.
- Quyền riêng tư: VPN che giấu địa chỉ IP, giúp bạn ẩn danh khi trực tuyến. Điều này giúp bảo vệ quyền riêng tư khỏi những người theo dõi trực tuyến.
- Truy cập nội dung: VPN cho phép truy cập các trang web và dịch vụ bị chặn về mặt địa lý. Ví dụ: nếu đang ở Việt Nam, có thể sử dụng VPN để truy cập các trang web chỉ có sẵn ở Hoa Kỳ.
- Bảo mật Wi-Fi công cộng: Wi-Fi công cộng thường không an toàn và có thể dễ dàng bị tấn công. Sử dụng VPN có thể giúp bảo vệ dữ liệu khỏi bị đánh cắp khi sử dụng Wi-Fi công cộng.
- Vượt qua kiểm duyệt internet: Một số quốc gia kiểm duyệt internet và chặn quyền truy cập vào các trang web và dịch vụ nhất định. VPN cho phép vượt qua kiểm duyệt internet và truy cập các trang web mong muốn.
- An toàn khi làm việc từ xa: Truy cập an toàn vào mạng nội bộ công ty từ xa.

1.7.2 Nhược điểm:

- Tốc độ: VPN có thể làm chậm kết nối internet vì lưu lượng truy cập phải được định tuyến qua máy chủ VPN.
- Chi phí: Một số VPN miễn phí, nhưng nhiều VPN tốt nhất là dịch vụ trả phí.
- Khả năng tương thích: Một số thiết bị hoặc dịch vụ không hỗ trợ sử dụng VPN hoặc VPN bị chặn ở một số quốc gia.
- Sự phức tạp: Cài đặt và sử dụng VPN có thể phức tạp đối với một số người dùng.

- **Rủi ro bảo mật:** Không phải tất cả các VPN đều được tạo ra như nhau. Một số dịch vụ VPN miễn phí hoặc không đáng tin cậy có thể lưu trữ, bán dữ liệu người dùng hoặc chứa phần mềm độc hại

1.8 Cách thiết lập mạng VPN

Cách thiết lập mạng VPN tùy vào từng trường hợp cụ thể như sau:

1.8.1 Sử dụng nhà cung cấp dịch vụ VPN

Người dùng có thể sử dụng dịch vụ VPN thông qua các phương pháp sau:

- **Trình duyệt web:** Một số nhà cung cấp dịch vụ VPN cho phép người dùng truy cập vào mạng VPN thông qua trình duyệt web. Người dùng chỉ cần truy cập vào trang web của nhà cung cấp, đăng nhập và kích hoạt kết nối VPN trực tiếp từ trình duyệt.
- **Ứng dụng, phần mềm:** Nhiều nhà cung cấp VPN cũng cung cấp ứng dụng hoặc phần mềm dành riêng cho các thiết bị di động, máy tính để bàn hoặc các nền tảng khác. Người dùng có thể tải xuống và cài đặt ứng dụng VPN trên thiết bị của mình, sử dụng để kết nối và quản lý các kết nối VPN.
- **Đăng ký theo gói:** Các dịch vụ VPN thường cung cấp các gói dịch vụ khác nhau cho người dùng lựa chọn. Người dùng có thể đăng ký và lựa chọn gói phù hợp với nhu cầu của họ. Thông thường, dịch vụ VPN tính phí dựa trên mỗi thiết bị sử dụng, tuy nhiên, cũng có những gói dịch vụ có giá trị cao hơn cho các tính năng và quyền hạn sử dụng bổ sung.

1.8.2 Sử dụng bộ định tuyến VPN

Sử dụng bộ định tuyến VPN có thể được thực hiện như sau:

- **Mua bộ định tuyến VPN:** Người dùng có thể mua một bộ định tuyến đã được cài đặt và kết nối VPN sẵn từ nhà cung cấp. Bộ định tuyến này đã được cấu hình để tự động kết nối và bảo vệ toàn bộ mạng thông qua VPN. Người dùng chỉ cần cắm bộ định tuyến vào mạng và cung cấp các thông tin đăng nhập VPN để kích hoạt kết nối.
- **Cài đặt phần mềm VPN trên bộ định tuyến:** Người dùng có thể tự cài đặt phần mềm VPN lên bộ định tuyến tại nhà. Thông thường, các nhà cung cấp dịch vụ VPN cung cấp hướng dẫn cài đặt và cấu hình cho các bộ định tuyến phổ biến. Sau khi cài đặt, bộ định tuyến sẽ tự động kết nối và bảo vệ toàn bộ mạng thông qua VPN.

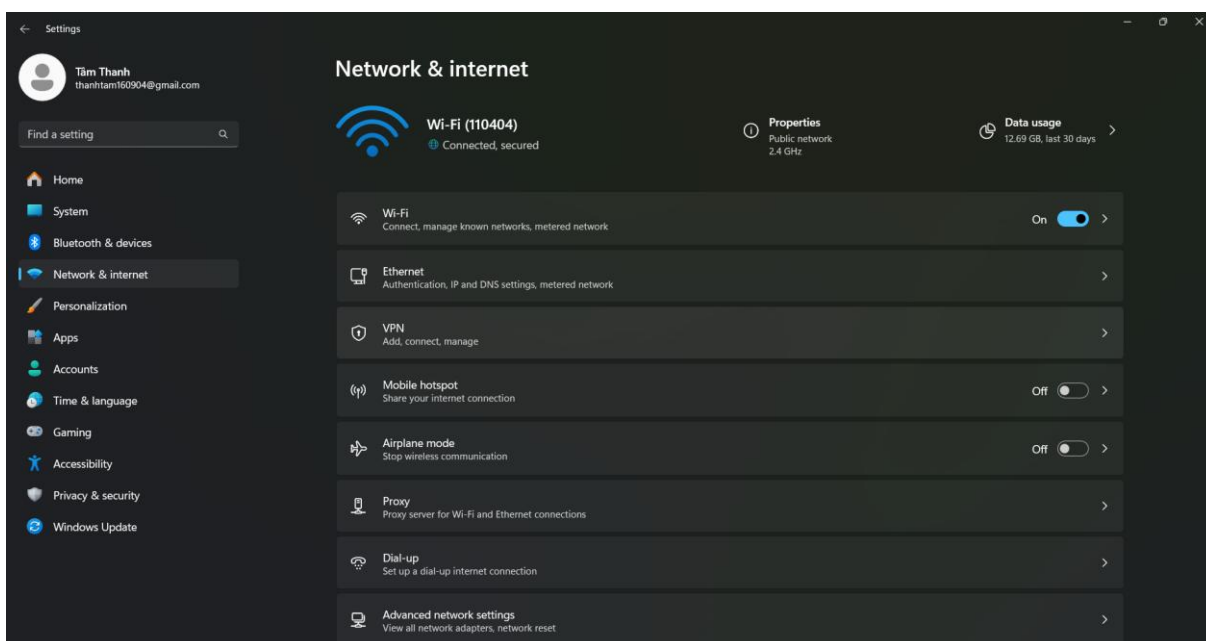


Hình 8 Thiết bị phát sóng Wi-Fi (Router) trong mạng nội bộ

1.8.3 Hướng dẫn cài đặt và sử dụng VPN đơn giản

Việc cài đặt và sử dụng VPN tương đối đơn giản, sau đây sẽ hướng dẫn các bước thực hiện trên máy tính chạy Windows 11:

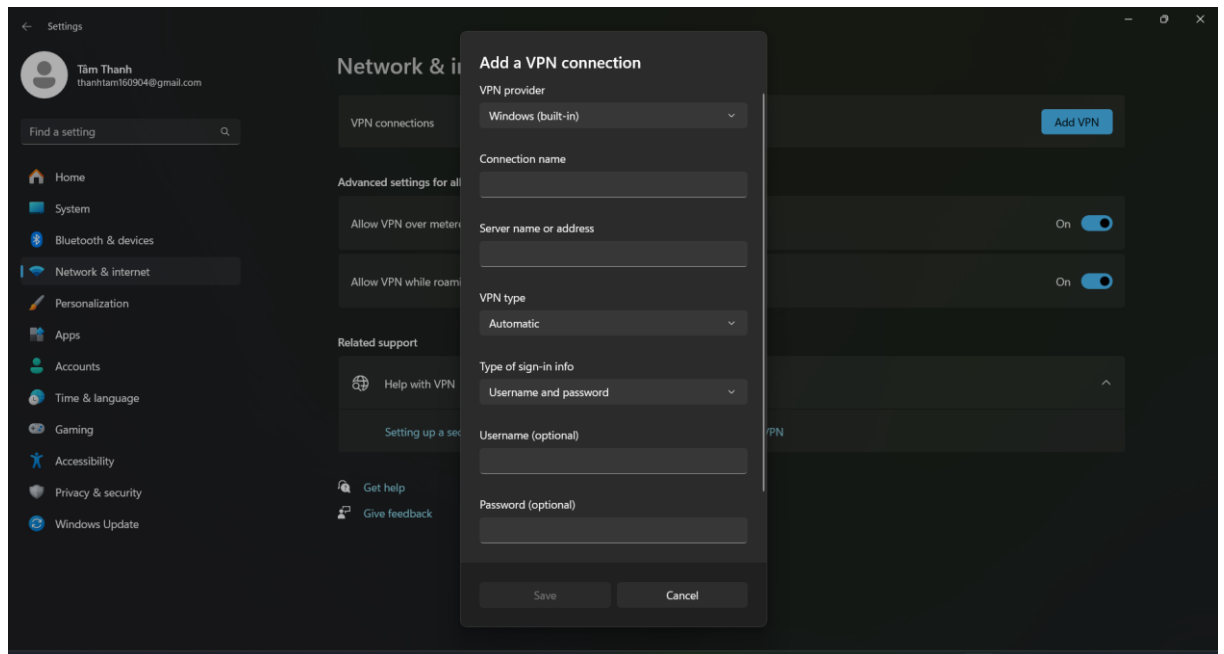
- Bước 1: Tại mục Start, bạn chọn vào Settings, sau đó nhấn chọn Network & internet.



Hình 9 Hướng dẫn cài đặt và sử dụng VPN đơn giản

- Bước 2: Tại mục Network & internet, bạn chọn vào phần VPN và nhấn chọn Add VPN.
- Bước 3: Sau khi kết nối xong, giao diện truy cập như trong hình. Tại thời điểm này, bạn cần chọn VPN Provider. Sau đó, nhập thông tin mạng ảo và địa chỉ máy chủ sẽ được truy cập.

Lưu ý: Trong phần VPN type, có thể tùy chọn khu vực địa lý sao cho phù hợp với nhu cầu truy cập.



Hình 10 Hướng dẫn cài đặt và sử dụng VPN đơn giản

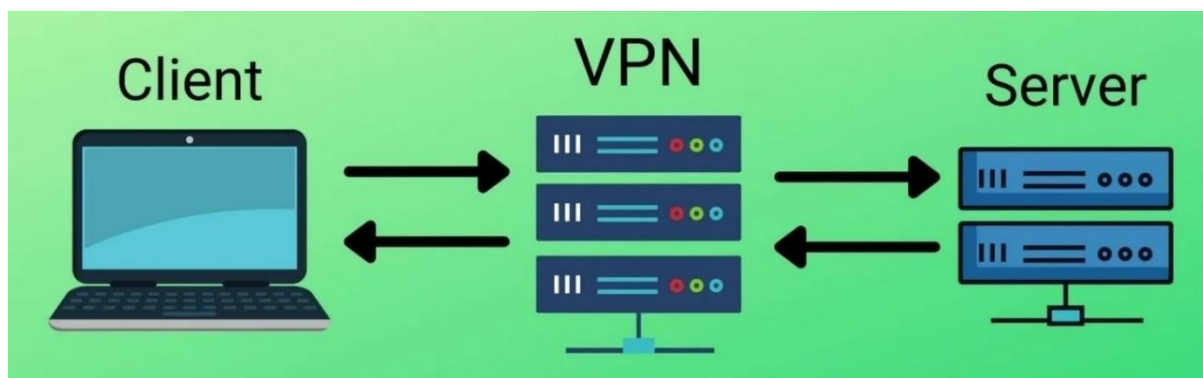
1.9 Kết chương

Chương 1 đã khái quát rõ ràng về VPN: từ định nghĩa, chức năng, cách hoạt động cho đến ưu – nhược điểm và ứng dụng thực tiễn. Thông qua phần này, người đọc có thể hiểu được tầm quan trọng của VPN trong bảo vệ dữ liệu cá nhân, tổ chức cũng như vai trò của các mô hình kết nối trong thực tế.

CHƯƠNG 2. CẤU TRÚC VÀ GIAO THỨC TRONG VPN

2.1 Cấu trúc và cách thức hoạt động

Một mô hình VPN có kiến trúc tương tự như 1 mô hình client-server thông thường, nó được cấu thành bởi 3 thành phần: VPN Server, VPN Client và VPN Tunnel.



Hình 11 Mô hình VPN đơn giản

2.1.1 VPN Server

VPN server là một máy chủ được cài đặt và cấu hình bởi các phần mềm VPN server, có chức năng xử lý các yêu cầu kết nối được thực hiện bởi các VPN client từ xa hoặc các VPN client cục bộ, cung cấp các thuật toán mã hóa dữ liệu. Nó hoạt động như cái cổng kết nối giữa các VPN client và mạng riêng. Các VPN client trước khi được cấp quyền truy cập vào mạng riêng thì phải tự xác thực trước với VPN server.

Đối với các mạng lớn, có lưu lượng cao thì cần nhiều hơn một VPN server để tránh gây ra độ trễ không đáng có. Một VPN server sẽ có 2 giao diện, một là giao diện đối với mạng LAN nội bộ và một giao diện khác đối với Internet.

2.1.2 VPN Client

VPN client có chức năng gửi yêu cầu kết nối đến VPN Server, đóng vai trò là trung gian giữa end users và server, thực hiện mã hóa dữ liệu của end users theo thuật toán được phía VPN Server yêu cầu.

Nó có thể là các thiết bị từ xa được người dùng kết nối đến mạng POP nội bộ của tổ chức hoặc là các thiết bị thuộc mạng cục bộ (LAN) của tổ chức.

2.1.3 VPN Tunnel

VPN Tunnel cung cấp các kết nối logic, điểm tới điểm vận chuyển các gói dữ liệu mã hóa bằng một đường hầm riêng biệt qua mạng IP, điều đó làm tăng tính

bảo mật thông tin vì dữ liệu sau khi mã hóa sẽ lưu chuyển trong một đường hầm được thiết lập giữa người gửi và người nhận cho nên sẽ tránh được sự mất cắp, xem trộm thông tin, đường hầm chính là đặc tính ảo của VPN.

2.2 Phân loại VPN

2.2.1 VPN truy cập từ xa(Remote Access VPN)

Mạng riêng ảo (VPN) truy cập từ xa cho phép người dùng đang làm việc từ xa truy cập an toàn vào các ứng dụng và dữ liệu lưu trữ tại trung tâm dữ liệu và trụ sở chính của công ty, mã hóa mọi lưu lượng mà người dùng gửi và nhận.

VPN truy cập từ xa an toàn tạo ra một đường hầm giữa mạng và người dùng từ xa, gần như là riêng tư. Lưu lượng được mã hóa, khiến những kẻ nghe lén không thể hiểu được. Người dùng ở các vị trí xa có thể truy cập và sử dụng mạng một cách an toàn theo cách tương tự như ở văn phòng. Sử dụng VPN truy cập từ xa, dữ liệu có thể được truyền đi mà không có nguy cơ bị chặn hoặc giả mạo.



Hình 12 Mô hình VPN truy cập từ xa(Remote Access VPN)

VPN truy cập từ xa hoạt động bằng cách thiết lập kết nối được mã hóa an toàn từ thiết bị của người dùng đến mạng công ty. Quá trình này bắt đầu với máy khách VPN quản lý quá trình xác thực ban đầu, xác nhận rằng chỉ những người dùng được ủy quyền mới có thể thiết lập kết nối. Sau khi xác thực, phần mềm máy khách VPN tạo đường hầm được mã hóa đến cổng VPN. Cổng hoạt động như máy chủ VPN, tạo điều kiện cho đường dẫn an toàn để truyền dữ liệu.

Ngay cả trên các mạng internet công cộng, tất cả dữ liệu được truyền qua đường hầm đều được mã hóa, bảo toàn tính bảo mật và toàn vẹn của dữ liệu. Đường hầm an toàn mở rộng phạm vi mạng đến người dùng từ xa, về cơ bản là đặt họ trong mạng công ty. Quy trình này cho phép truy cập an toàn vào các tài nguyên nội bộ như ứng dụng, máy chủ tệp và cơ sở dữ liệu.

VPN từ xa thường bao gồm các tính năng bảo mật bao gồm xác thực đa yếu tố và các tiêu chuẩn mã hóa nâng cao. Các lớp bảo mật bổ sung đảm bảo kết nối vẫn riêng tư và bảo vệ mạng công ty khỏi các mối đe dọa tiềm ẩn do các thiết bị từ xa gây ra.

Lợi ích của VPN truy cập từ xa:

- **Kết nối từ xa an toàn:** VPN truy cập từ xa bảo mật kết nối đến mạng công ty cho người làm việc từ xa và người dùng di động. Nó mã hóa lưu lượng dữ liệu, đảm bảo tính bảo mật và bảo vệ tính toàn vẹn của thông tin nhạy cảm.
- **Có khả năng tiết kiệm chi phí:** Việc triển khai VPN truy cập từ xa đôi khi có thể là giải pháp tiết kiệm chi phí để mở rộng quyền truy cập mạng vượt ra ngoài phạm vi vật lý của văn phòng. Đối với một số công ty, nó có thể trì hoãn nhu cầu ban đầu về đầu tư cơ sở hạ tầng mở rộng.
- **Quản lý đơn giản:** VPN truy cập từ xa đơn giản hóa việc quản lý mạng bằng cách cung cấp một điểm kiểm soát duy nhất cho quyền truy cập của người dùng và các chính sách bảo mật. Người quản trị có thể dễ dàng quản lý các kết nối, giám sát bảo mật và thực thi các chính sách mà không cần cấu hình phức tạp tại chỗ.

Thách thức của VPN truy cập từ xa:

Theo truyền thống, VPN truy cập từ xa là một yếu tố chính trong việc cung cấp cho nhân viên từ xa quyền truy cập vào các nguồn lực của công ty. Tuy nhiên, khi kiến trúc mạng phát triển và các mối đe dọa bảo mật trở nên tinh vi hơn, các VPN này đôi khi có thể gây ra thách thức, đặc biệt là khi so sánh với các giải pháp hiện đại hơn.

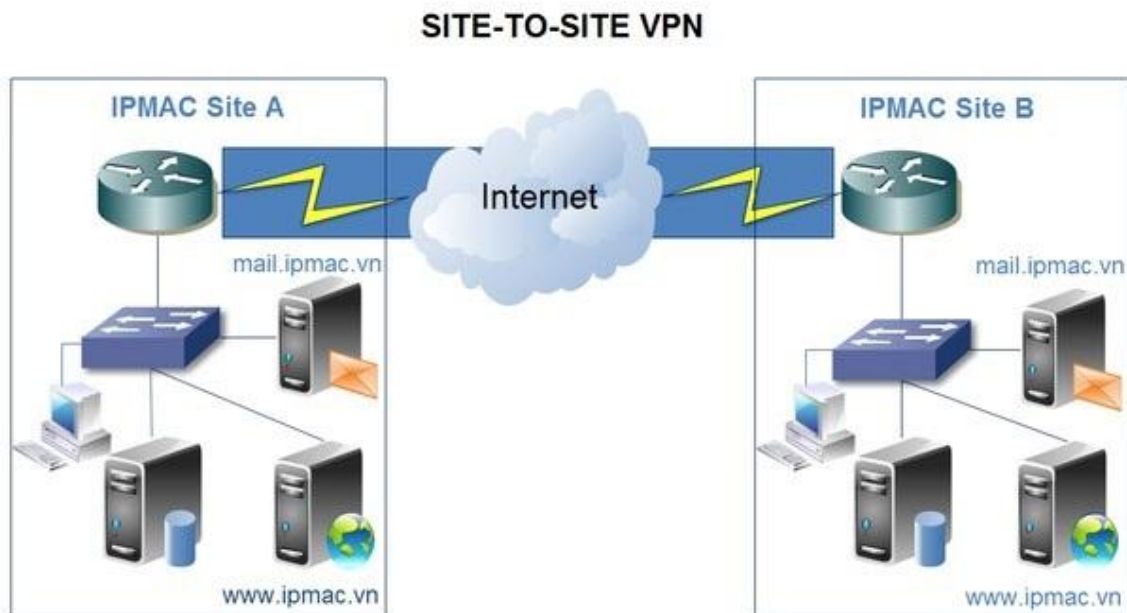
- **Biện pháp an ninh hạn chế:** VPN truy cập từ xa truyền thống không cung cấp đủ các biện pháp kiểm soát bảo mật ngoài các biện pháp cơ bản về mã hóa và xác thực. Chúng có thể thiếu khả năng thực thi các biện pháp kiểm soát truy

cập chi tiết, khiến các tài nguyên nhạy cảm của công ty có khả năng bị truy cập trái phép.

- Trải nghiệm người dùng không nhất quán: Trải nghiệm người dùng với VPN truy cập từ xa có thể không nhất quán và đôi khi chùng kèn, tùy thuộc vào nhà cung cấp và nền tảng. Các vấn đề về kết nối và nhu cầu đăng nhập thủ công có thể cản trở năng suất và gây khó chịu cho nhân viên từ xa.
- Quản lý phức tạp và khả năng mở rộng: Khi các tổ chức phát triển, việc quản lý VPN truy cập từ xa có thể trở nên phức tạp và tốn thời gian. Việc mở rộng quy mô để đáp ứng số lượng người dùng làm việc từ xa ngày càng tăng thường đòi hỏi phần cứng bổ sung và có thể dẫn đến chi phí quản lý đáng kể.
- Tiếp xúc với lỗ hổng mạng: VPN truy cập từ xa có thể khiến mạng dễ bị tấn công, đặc biệt là nếu thiết bị đầu cuối bị xâm phạm. Vì VPN thường không đánh giá trạng thái bảo mật của thiết bị nên chúng có thể vô tình trở thành đường dẫn cho phần mềm độc hại hoặc các mối đe dọa mạng khác.

2.2.2 Mạng VPN cục bộ (Intranet-based VPN)

Các VPN cục bộ được sử dụng để bảo mật các kết nối giữa các địa điểm khác nhau của một công ty. Mạng VPN liên kết trụ sở chính, các văn phòng, chi nhánh trên một cơ sở hạ tầng chung sử dụng các kết nối luôn được mã hoá bảo mật. Điều này cho phép tất cả các địa điểm có thể truy cập an toàn các nguồn dữ liệu được phép trong toàn bộ mạng của công ty. Những VPN này vẫn cung cấp những đặc tính của mạng WAN như khả năng mở rộng, tính tin cậy và hỗ trợ cho nhiều kiểu giao thức khác nhau với chi phí thấp nhưng vẫn đảm bảo tính mềm dẻo. Kiểu VPN này thường được cấu hình như là một VPN Site- to- Site.



Hình 13 Mô hình VPN Site-to-Site (Intranet Based)

Những ưu điểm chính của mạng cục bộ dựa trên giải pháp VPN bao gồm:

- Các mạng lưới cục bộ hay toàn bộ có thể được thiết lập (với điều kiện mạng thông qua một hay nhiều nhà cung cấp dịch vụ).
- Giảm được số nhân viên kỹ thuật hỗ trợ trên mạng đối với những nơi xa.
- Bởi vì những kết nối trung gian được thực hiện thông qua mạng Internet, nên nó có thể dễ dàng thiết lập thêm một liên kết ngang cấp mới.
- Tiết kiệm chi phí thu được từ những lợi ích đạt được bằng cách sử dụng đường ngầm VPN thông qua Internet kết hợp với công nghệ chuyển mạch tốc độ cao. Ví dụ như công nghệ Frame Relay, ATM.

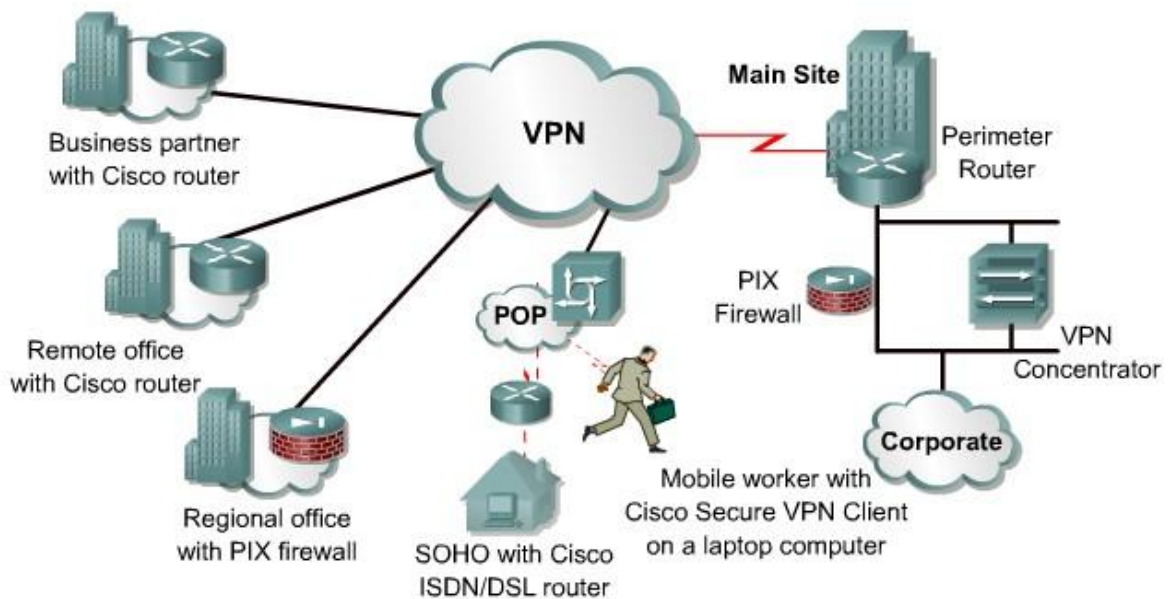
Tuy nhiên mạng cục bộ dựa trên giải pháp VPN cũng có những nhược điểm đi cùng như:

- Bởi vì dữ liệu được truyền “ngầm” qua mạng công cộng – mạng Internet – cho nên vẫn còn những mối “đe dọa” về mức độ bảo mật dữ liệu và mức độ chất lượng dịch vụ (QoS).
- Khả năng các gói dữ liệu bị mất trong khi truyền dẫn vẫn còn khá cao.
- Trường hợp truyền dẫn khối lượng lớn dữ liệu, như là đa phương tiện, với yêu cầu truyền dẫn tốc độ cao và đảm bảo thời gian thực là thách thức lớn trong môi trường Internet.

2.2.3 2. Mạng VPN mở rộng (Extranet-based VPN)

Thực tế mạng VPN mở rộng cung cấp khả năng điều khiển truy nhập tới những nguồn tài nguyên mạng cần thiết để mở rộng những đối tượng kinh doanh

như là các đối tác, khách hàng, và các nhà cung cấp... . Các VPN mở rộng cung cấp một đường hầm bảo mật giữa các khách hàng, các nhà cung cấp và các đối tác qua một cơ sở hạ tầng công cộng. Kiểu VPN này sử dụng các kết nối luôn luôn được bảo mật và được cấu hình như một VPN Site-to-Site. Sự khác nhau giữa một VPN cục bộ và một VPN mở rộng đó là sự truy cập mạng được công nhận ở một trong hai đầu cuối của VPN.



Hình 14 Mô hình VPN Site-to-Site (Extranet-Based VPN)

Những ưu điểm chính của mạng VPN mở rộng:

- Chi phí cho mạng VPN mở rộng thấp hơn rất nhiều so với mạng truyền thống.
- Dễ dàng thiết lập, bảo trì và dễ dàng thay đổi đối với mạng đang hoạt động.
- Vì mạng VPN mở rộng được xây dựng dựa trên mạng Internet nên có nhiều cơ hội trong việc cung cấp dịch vụ và chọn lựa giải pháp phù hợp với các nhu cầu của mỗi công ty hơn.
- Bởi vì các kết nối Internet được nhà cung cấp dịch vụ Internet bảo trì, nên giảm được số lượng nhân viên kỹ thuật hỗ trợ mạng, do vậy giảm được chi phí vận hành của toàn mạng.

Bên cạnh những ưu điểm ở trên giải pháp mạng VPN mở rộng cũng còn những nhược điểm đi cùng như:

- Khả năng bảo mật thông tin, mất dữ liệu trong khi truyền qua mạng công cộng vẫn tồn tại.

- Truyền dẫn khối lượng lớn dữ liệu, như là đa phương tiện, với yêu cầu truyền dẫn tốc độ cao và đảm bảo thời gian thực, là thách thức lớn trong môi trường Internet.
- Làm tăng khả năng rủi ro đối với các mạng cục bộ của công ty.

2.2.4 VPN truy cập từ xa so với VPN Site-to-Site

- Sự khác biệt chính giữa VPN site-to-site và VPN truy cập từ xa là kiến trúc kết nối mạng và trường hợp sử dụng.
- VPN site-to-site liên kết toàn bộ mạng với nhau. Chúng bảo mật lưu lượng ở rìa mạng, cho phép các site khác nhau chia sẻ tài nguyên như thể chúng là một phần của cùng một mạng.
- VPN truy cập từ xa phục vụ cho người dùng cá nhân muốn truy cập mạng từ các vị trí xa. Các VPN này sử dụng phần mềm máy khách được cài đặt trên thiết bị của mỗi người dùng để tạo đường hầm an toàn đến mạng.

2.3 Các giao thức đường hầm phổ biến

2.3.1 Giao thức chuyển tiếp lớp 2 (L2F – Layer Two Forwarding)

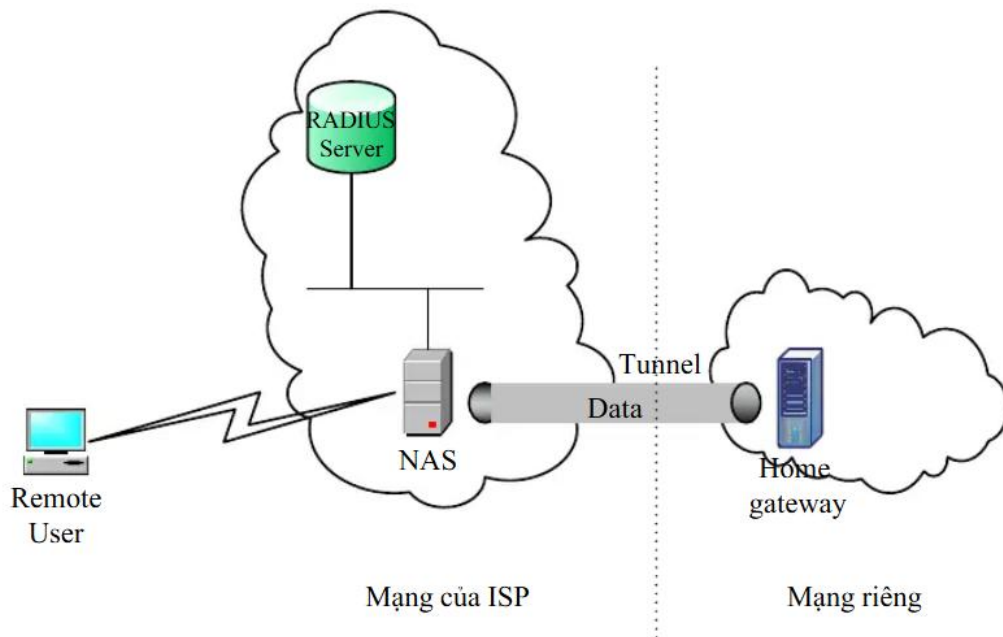
L2F là một giao thức cho phép tạo Mạng riêng ảo (VPN) . Cisco Systems đã phát triển giao thức này để thiết lập VPN qua internet hoặc các mạng dựa trên IP khác. Thuật ngữ "Lớp 2" dùng để chỉ lớp thứ hai của mô hình Kết nối hệ thống mở (OSI), được gọi là Lớp liên kết dữ liệu.

2.3.1.1 Cách thức hoạt động của chuyển tiếp lớp 2

Hoạt động của Layer 2 Forwarding tương đối đơn giản. Nó bao gồm việc đóng gói các khung dữ liệu để truyền qua mạng IP. L2F không cung cấp mã hóa, nhưng nó cho phép dữ liệu được gửi an toàn qua internet bằng cách tạo một đường hầm giữa mạng của người dùng từ xa và trang web trung tâm. Sau đó, các khung dữ liệu có thể được chuyển tiếp dọc theo đường hầm này để đến đích.

1bit	1bit	1bit	1bit	8bit	1bit	3bit	8bit	8bit
F	K	P	S	Reserved	C	Versi on	Protocol	Sequence
Multiplex ID							Client ID	
Length							Offset	
Key								
Data								
Checksum								

Hình 15 Cấu trúc gói của giao thức L2F



Hình 16 Mô hình hệ thống của giao thức L2F

2.3.1.2 Ưu điểm của chuyển tiếp lớp 2

- Hiệu quả: L2F cung cấp một cách hiệu quả để vận chuyển các gói dữ liệu qua Internet bằng cách thiết lập một đường hầm an toàn giữa hai mạng, nâng cao tốc độ và độ tin cậy của việc truyền dữ liệu.
- Bảo mật: Bằng cách tạo ra mạng riêng ảo, L2F đảm bảo dữ liệu được truyền qua internet được an toàn và riêng tư, bảo vệ dữ liệu khỏi các mối đe dọa mạng tiềm ẩn.
- Tính linh hoạt: L2F thể hiện tính linh hoạt của mình bằng cách thích ứng với nhiều ứng dụng khác nhau, từ việc tạo VPN cho ISP đến truyền tải khung PPP, đáp ứng hiệu quả nhiều nhu cầu mạng khác nhau.

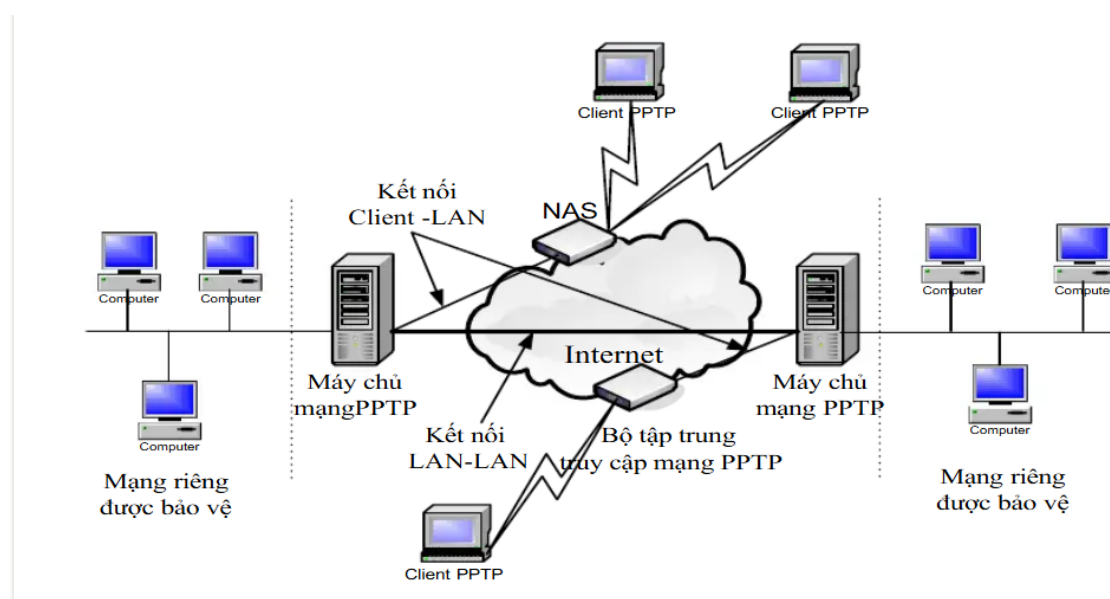
2.3.1.3 Nhược điểm của chuyển tiếp lớp 2

- Thiếu mã hóa: Chuyển tiếp lớp 2 về cơ bản không cung cấp bất kỳ mã hóa nào, khiến dữ liệu dễ bị chặn và sửa đổi nếu không có các biện pháp bảo mật bổ sung.
- Phụ thuộc vào ISP: L2F yêu cầu các Nhà cung cấp dịch vụ Internet (ISP) đáng tin cậy để có hiệu suất tối ưu, nhưng không phải lúc nào cũng có sẵn hoặc ổn định, đặc biệt là ở các vùng nông thôn hoặc vùng sâu vùng xa.
- Độ phức tạp: Việc thiết lập và quản lý L2F có thể phức tạp và tốn thời gian, đòi hỏi trình độ chuyên môn kỹ thuật cao, đây có thể là rào cản đối với các tổ chức nhỏ hơn hoặc những tổ chức thiếu nhân viên kỹ thuật.

2.3.2 Giao thức đường hầm điểm tới điểm (PPTP - Point-To-Point Tunneling Protocol)

PPTP (Giao thức đường hầm điểm-điểm) là một giao thức mạng được sử dụng để thiết lập kết nối VPN an toàn qua Internet.

Giao thức đường hầm điểm-điểm tạo điều kiện thuận lợi cho việc truyền dữ liệu riêng tư từ máy khách từ xa đến máy chủ bằng cách đóng gói các gói tin ở cấp độ TCP/IP. Mặc dù có vai trò trong quá trình phát triển VPN ban đầu, PPTP đã phần lớn bị thay thế bởi các giao thức an toàn hơn do các lỗ hổng đã biết và tiêu chuẩn mã hóa yếu.



Hình 17 Hệ thống cung cấp VPN dựa trên PPTP

Giao thức đường hầm điểm-điểm (PPTP) thiết lập kết nối VPN bằng cách đóng gói các khung (PPP) trong các gói IP để truyền qua internet. Giao thức này hoạt động bằng cách sử dụng kênh điều khiển TCP và đường hầm đóng gói định tuyến chung (GRE). Sự kết hợp này cho phép giao thức đóng gói các gói PPP, giúp có thể sử dụng VPN trên nhiều mạng khác nhau.

Các cơ chế xác thực:

- PAP (Password Authentication Protocol) – giao thức xác thực mật khẩu
- CHAP (Challenge HandShake Authentication Protocol) – giao thức xác thực đòi hỏi bắt tay
- EAP (Extensible Authentication Protocol) – giao thức xác thực mở rộng

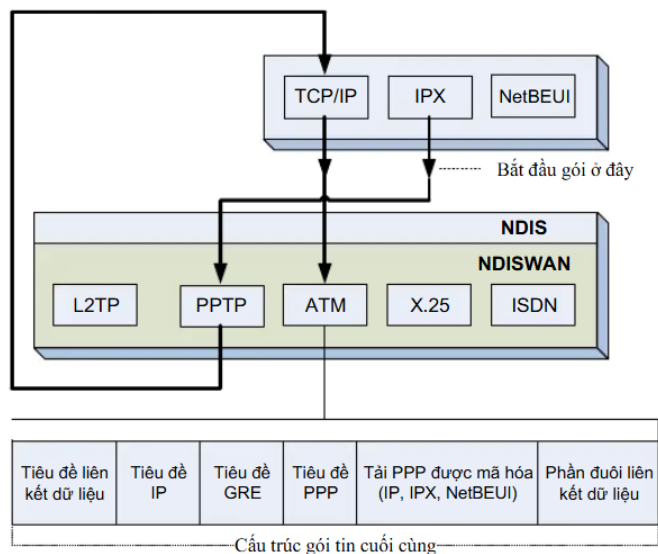
Tiêu đề liên kết dữ liệu	Tiêu đề IP	Tiêu đề TCP	Bản tin điều khiển PPTP	Phần đuôi liên kết dữ liệu
--------------------------	------------	-------------	-------------------------	----------------------------

Gói dữ liệu kết nối điều khiển PPTP

Tiêu đề liên kết dữ liệu	Tiêu đề IP	Tiêu đề GRE	Tiêu đề PPP	Tải PPP được mã hoá (IP, IPX, NetBEUI)	Phần đuôi liên kết dữ liệu
--------------------------	------------	-------------	-------------	----------------------------------------	----------------------------

Đóng gói dữ liệu đường hầm PPTP

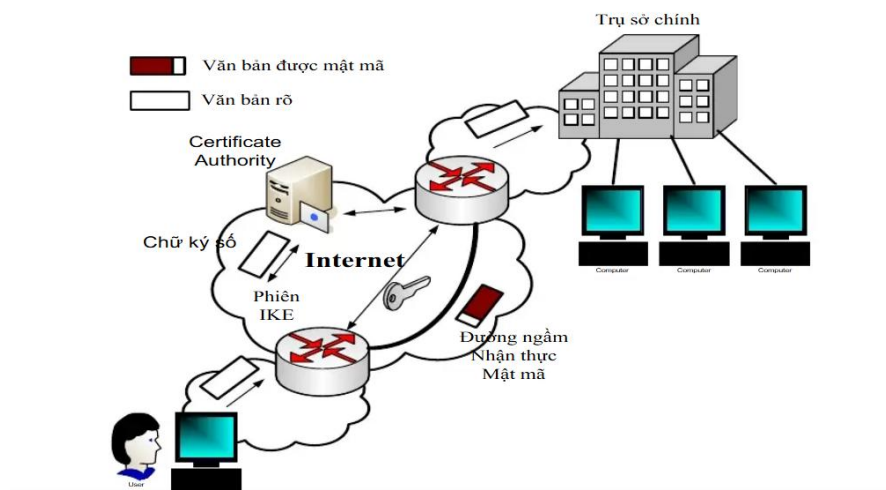
Hình 18 Cấu trúc gói PPTP



Hình 19 Sơ đồ đóng gói PPTP

2.3.3 Giao thức bảo mật IP (IPSec – Internet Protocol Security)

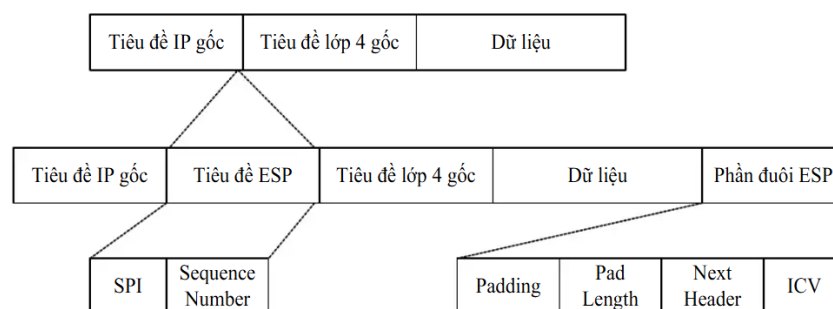
Internet Protocol Security (viết tắt IPSec) là một bộ giao thức mật mã tiêu chuẩn nhằm bảo vệ lưu lượng dữ liệu thông qua mạng internet Protocol (IP)



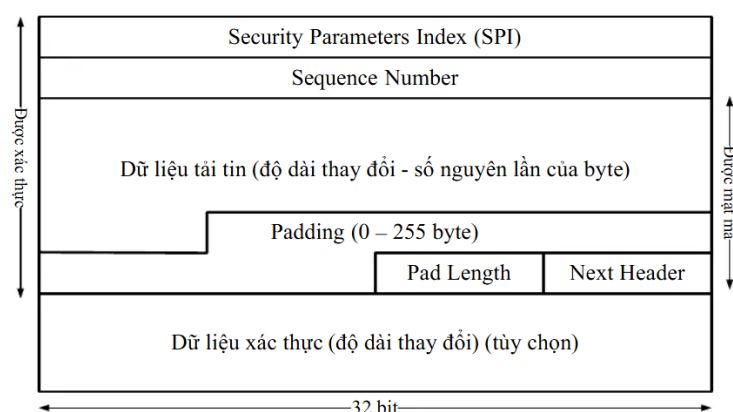
Hình 20 Mô hình sử dụng VPN trên nền IPSec

Các thành phần của IPSec bao gồm:

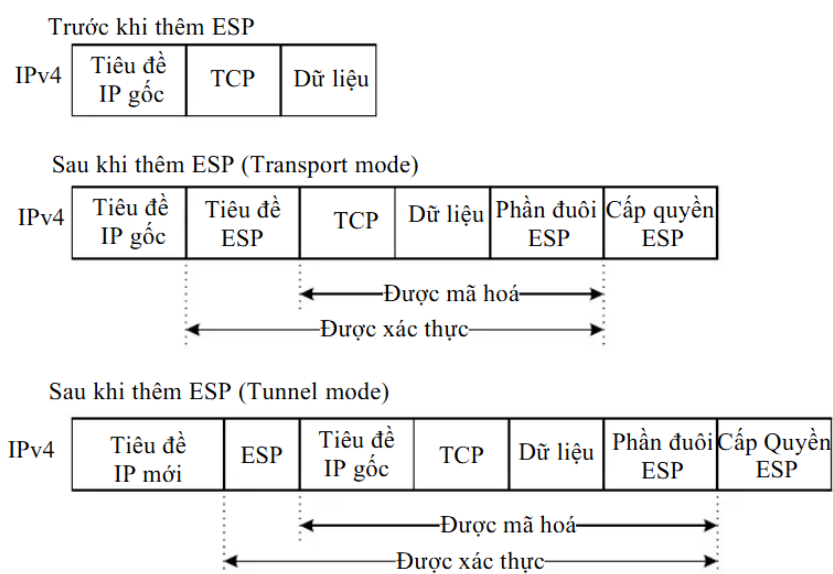
- Encapsulating Security Payload (ESP):
 - Giao thức ESP có trách nhiệm cung cấp phân mã hoá của IPSec, đảm bảo được độ bảo mật của lưu lượng dữ liệu giữa các thiết bị.
 - ESP vừa có nhiệm vụ mã hóa vừa phải xác thực các dữ liệu.



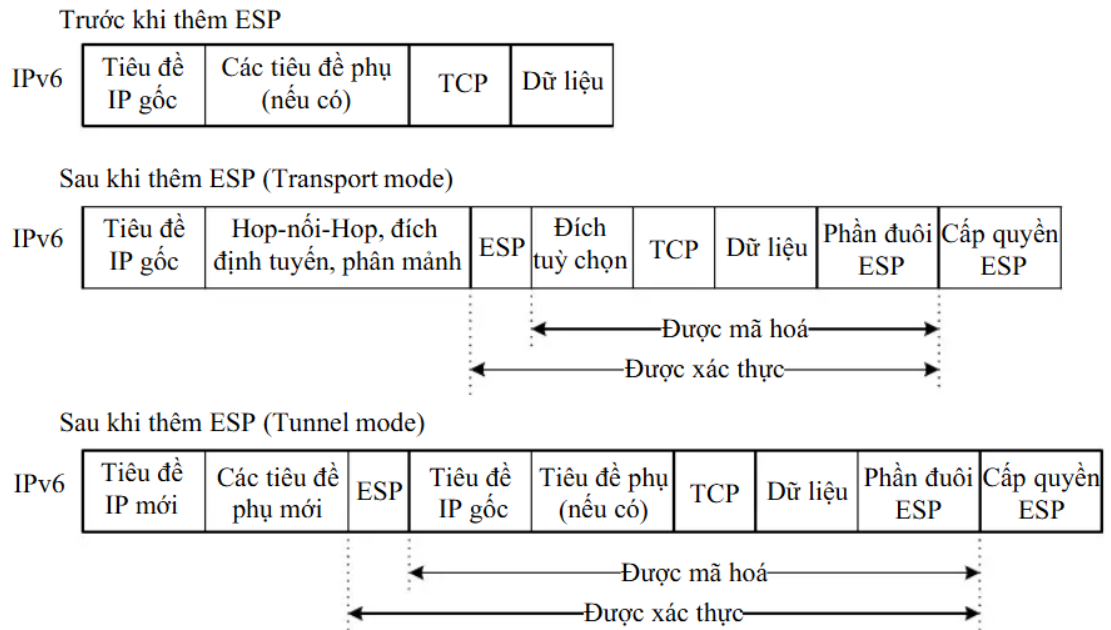
Hình 21 Cấu trúc tiêu đề ESP



Hình 22 Giao thức đóng gói tải tin an toàn ESP



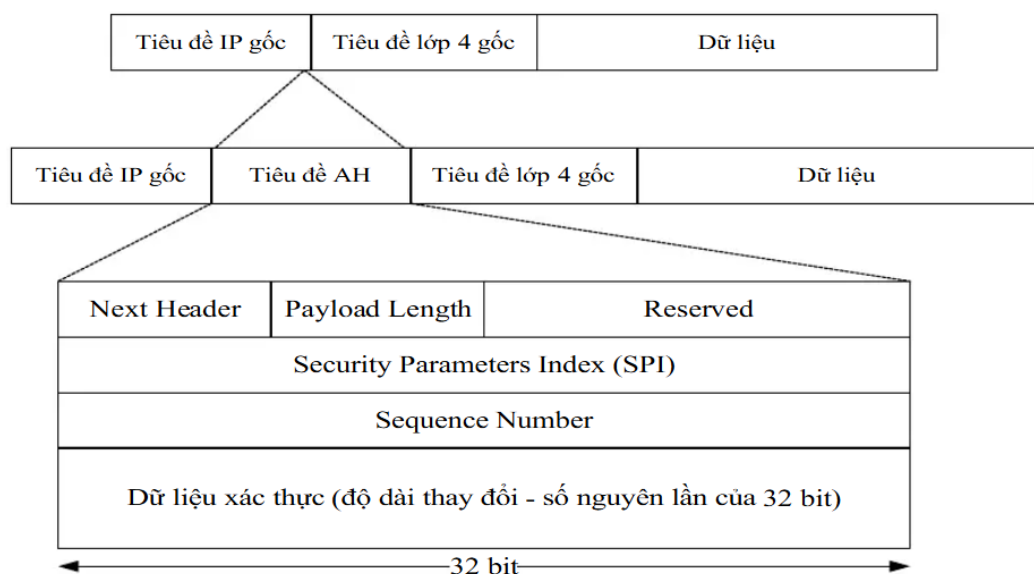
Hình 23 Khuôn dạng gói tin Ipv4 trước và sau khi xử lý ESP



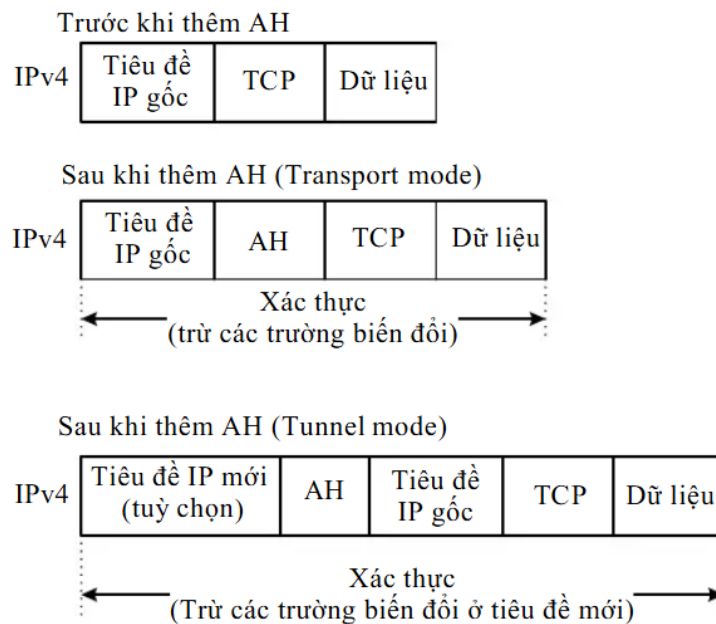
Hình 24 Khuôn dạng gói tin Ipv6 trước và sau khi xử lý ESP

▪ Authentication Header (AH):

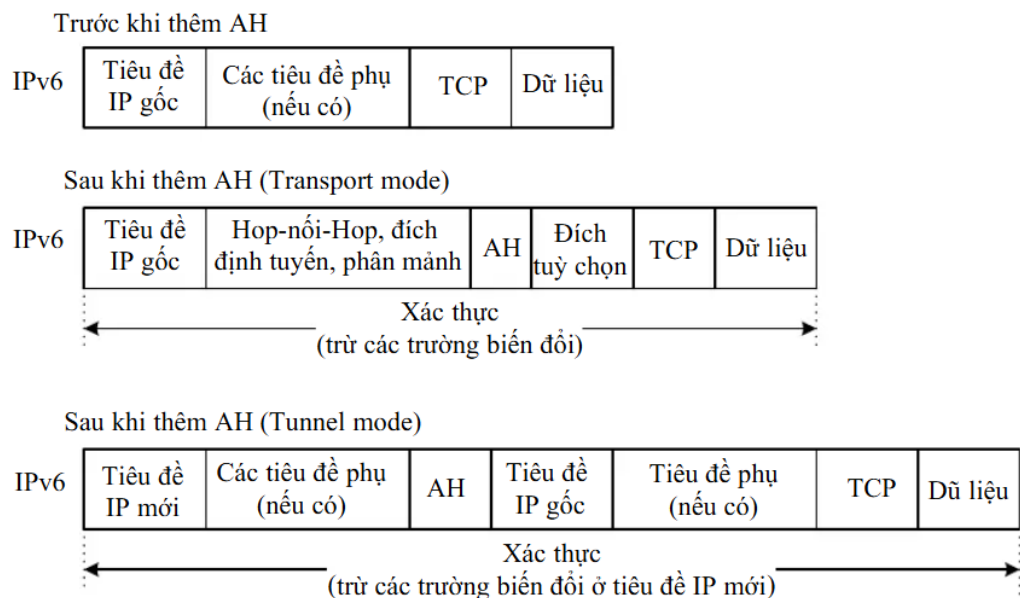
- Giao thức này có nhiệm vụ bảo vệ địa chỉ IP của các máy tính tham gia vào quá trình trao đổi thông tin nhằm đảm bảo các bit dữ liệu sẽ không bị mất, thay đổi hay bị hỏng trong quá trình truyền.
- AH cũng có nhiệm vụ xác minh rằng người gửi dữ liệu thực sự đã gửi nó, bảo vệ tunnel tránh sự xâm nhập của những người dùng trái phép.



Hình 25 Cấu trúc tiêu đề AH



Hình 26 Khuôn dạng gói tin Ipv4 trước và sau khi xử lý AH



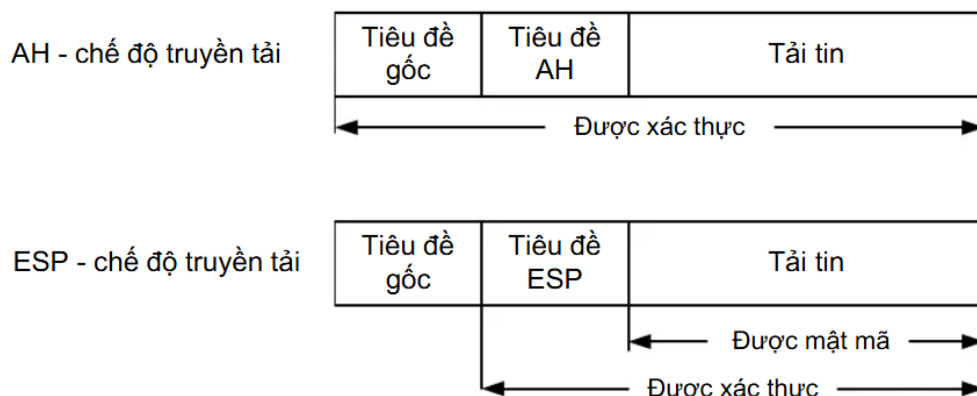
Hình 27 Khuôn dạng gói tin Ipv6 trước và sau khi xử lý AH

- Internet Key Exchange (IKE): IKE sẽ cho phép hai máy tính dễ dàng trao đổi và chia sẻ key mật mã một cách bảo mật khi thiết lập kết nối VPN.

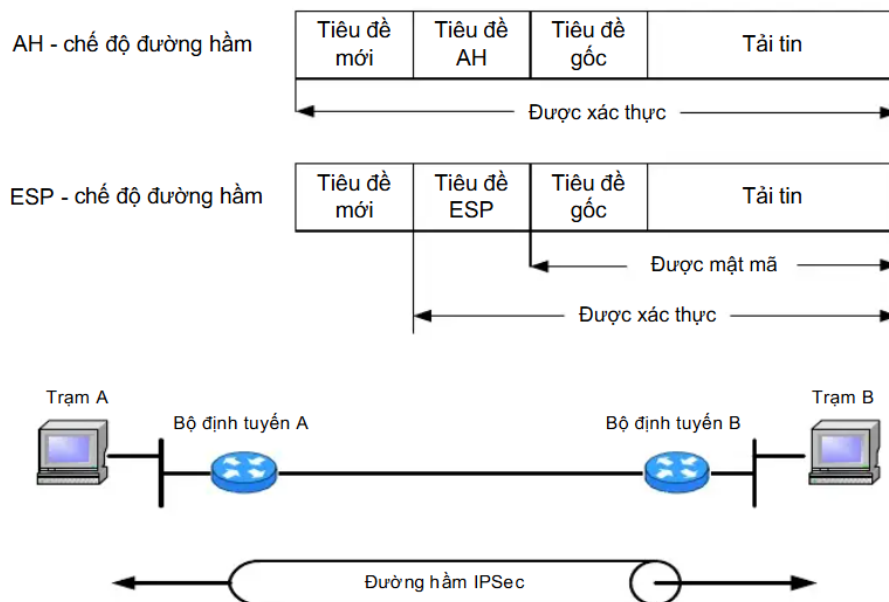
Có hai cơ chế hoạt động phổ biến của IPSec:

- Chế độ tunnel: Đối với chế độ này, toàn bộ gói tin được bảo vệ, bao gồm IP header. IPSec gói dữ liệu trong một packet mới, mã hoá nó và thêm một IP header mới. Nó thường được sử dụng trong thiết lập VPN site-to-site.

- Chế độ transport: Trong chế độ Transport, IP header không được mã hoá, chỉ có payload và ESP trailer được mã hoá. Chế độ Transport thường được sử dụng trong thiết lập VPN client-to-site.



Hình 28 Xử lý gói tin IP ở chế độ truyền tải



Hình 29 Xử lý gói tin IP ở chế độ đường hầm

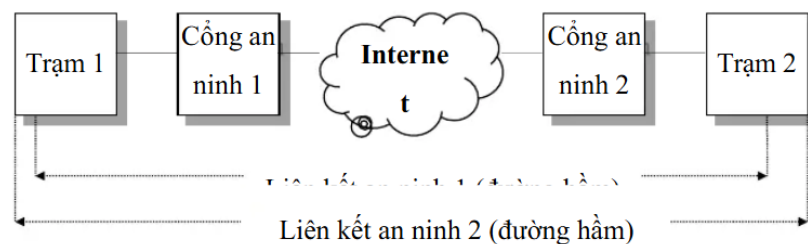
2.3.3.1 Liên kết an ninh và hoạt động trao đổi khóa:

Khái niệm

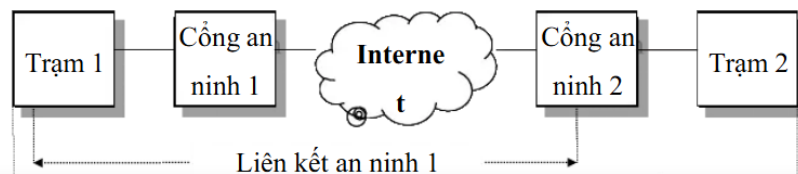
- Khi thiết lập kết nối IPSec, hai bên phải xác định các thuật toán sẽ được sử dụng, loại dịch vụ cần đảm bảo an ninh. Sau đó thương lượng để chọn các tham số và giải thuật áp dụng cho bảo mật hay xác thực.
- Dịch vụ bảo mật quan hệ giữa hai hay nhiều thực thể để thỏa thuận truyền thông an toàn được gọi là liên kết an ninh (SA – Security Association).
- SA là một kết nối đơn công. Với mỗi cặp truyền thông A và B có ít nhất hai SA (một từ A tới B và một từ B tới A).

- Khi lưu lượng cần truyền hai chiều qua VPN, giao thức trao đổi khóa IKE thiết lập một cặp SA trực tiếp, sau đó có thể thiết lập thêm nhiều SA khác.
- Mỗi SA có một thời gian sống riêng và được nhận dạng duy nhất bởi:
 - chỉ số thông số an ninh (SPI),
 - địa chỉ IP đích,
 - chỉ thị giao thức an ninh (AH hay ESP).
- Cơ chế quản lý SA của IPSec hiện nay chỉ được định nghĩa cho SA.

Kết hợp các SA kiểu đường hầm khi hai điểm cuối trùng nhau



Kết hợp các SA kiểu đường hầm khi một điểm cuối trùng nhau

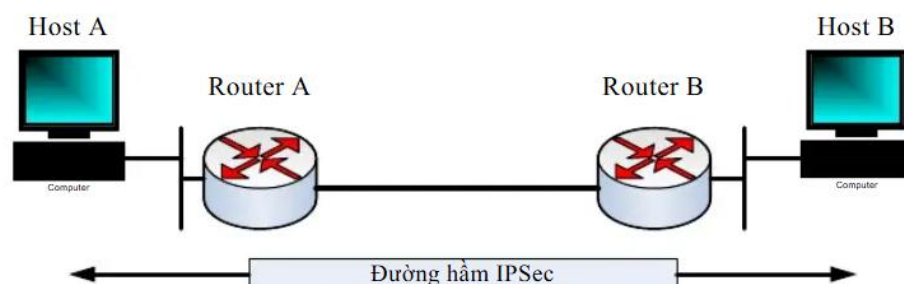


Hình 30 Kết hợp SA kiểu đường hầm khi hai hay một điểm cuối trùng nhau

Thiết lập kết nối IPSec:

- IPSec cung cấp việc xử lý ở mức gói,
- IKMP (Internet Key Management Protocol) chịu trách nhiệm thỏa thuận các SA.

IKE (Internet Key Exchange) được chọn là chuẩn để cấu hình SA cho IPSec.



Hình 31 Đường hầm IPSec được thiết lập

2.3.3.2 Một số vấn đề kỹ thuật trong thực hiện VPN trên nền IPSec

Thuật toán mã hóa (Encryption Algorithms):

- DES (Data Encryption Standard): chuẩn mã hóa cũ, hiện không còn an toàn trước các cuộc tấn công hiện đại.
- 3DES (Triple DES): cải tiến từ DES, mã hóa ba lần để tăng mức độ bảo mật.
- AES (Advanced Encryption Standard): chuẩn mã hóa hiện đại, mạnh mẽ và được sử dụng phổ biến trong VPN hiện nay.

Bảo đảm toàn vẹn bản tin (Data Integrity)

- HMAC (Hash-based Message Authentication Code): mã xác thực bản tin đảm bảo dữ liệu không bị thay đổi trong quá trình truyền.
- MD5 (Message Digest 5): thuật toán băm tóm gọn bản tin – hiện đã suy yếu trước các tấn công va chạm.
- SHA (Secure Hash Algorithm): thuật toán băm mạnh mẽ hơn, thường được dùng thay thế MD5.

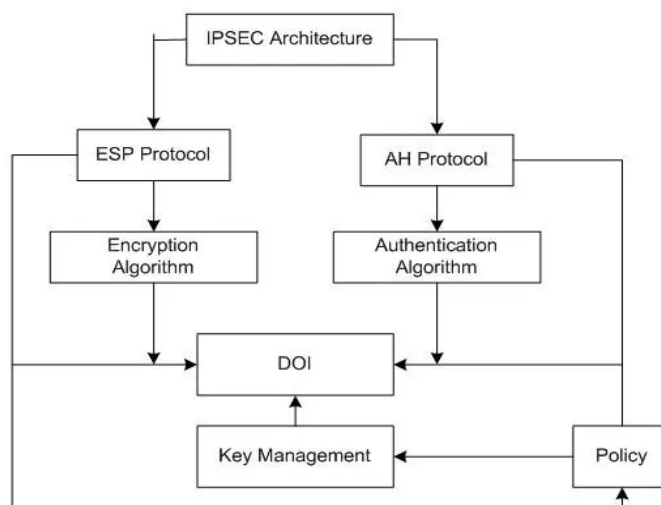
Xác thực các bên tham gia (Authentication Methods)

- Khóa chia sẻ trước (Pre-shared Keys – PSK): các bên dùng chung một khóa bí mật để xác thực.
- Chữ ký số RSA (RSA Digital Signatures): sử dụng cặp khóa công khai – riêng để xác thực danh tính.
- Nonce mã hóa bằng RSA (RSA-encrypted Nonces): dùng để ngăn chặn tấn công phát lại và xác minh tính mới của phiên giao tiếp.

2.3.3.3 Một số hạn chế kỹ thuật khi triển khai IPSec

- Gói tin IPSec có kích thước lớn hơn do phải bổ sung thêm các tiêu đề bảo mật như AH hoặc ESP, ảnh hưởng đến hiệu năng truyền tải.
- Giao thức IKE (Internet Key Exchange) hiện vẫn chưa chứng minh được đầy đủ mức độ ổn định và hiệu quả trong mọi môi trường triển khai.
- Phương thức trao đổi khóa thủ công không phù hợp với các hệ thống có số lượng lớn thiết bị di động do thiếu tính linh hoạt và khó quản lý.
- IPSec được thiết kế chỉ hỗ trợ lưu lượng IP, do đó không tương thích với các giao thức hoặc ứng dụng không sử dụng IP, hạn chế phạm vi ứng dụng.
- Việc xử lý các thuật toán mã hóa phức tạp gây tải nặng cho các máy tính có cấu hình thấp hoặc trạm làm việc hiệu năng hạn chế.

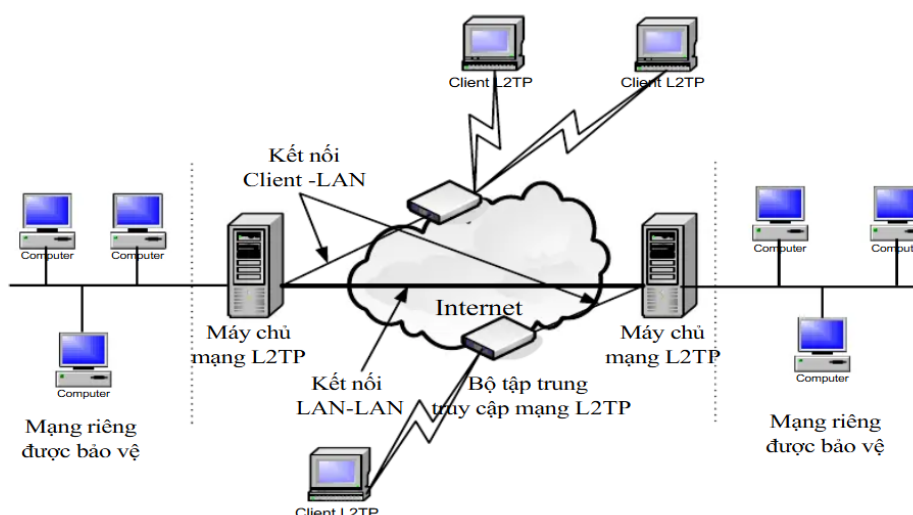
- Phân phối phần cứng/phần mềm mã hóa vẫn bị hạn chế ở một số quốc gia do các quy định kiểm soát xuất khẩu và bảo mật quốc gia.



Hình 32 Kiến trúc của IPsec

2.3.3.4 Giao thức đường hầm lớp 2 (L2TP – Layer Two Tunneling Protocol)

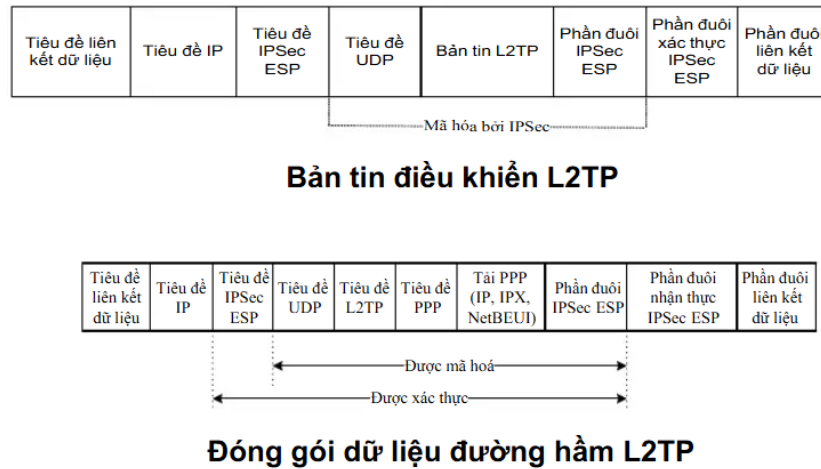
Giao thức đường hầm lớp 2 (L2TP) là giao thức tạo đường hầm an toàn để gửi dữ liệu giữa hai điểm trong mạng. Mặc dù nó không mã hóa dữ liệu riêng lẻ, nhưng nó thường được ghép nối với các giao thức mã hóa như IPsec. L2TP chủ yếu được sử dụng trong VPN để bảo mật kết nối qua mạng công cộng.



Hình 33 Hệ thống cung cấp VPN dựa trên L2TP

L2TP trên thực tế được biết đến với hiệu năng bảo mật cao hơn PPTP đáng kể. Tuy vậy, lỗ hổng của giao thức này nằm ở public key (khóa công khai). Thiết bị gửi và thiết bị nhận trao đổi và thỏa thuận về khóa mã hóa kế tiếp và không bên nào được biết mã này được gọi là public key Diffie-Hellman. Chỉ cần sức mạnh

điện toán đạt mức phù hợp sẽ mở được khoá và được quyền truy cập vào một VPN cụ thể.

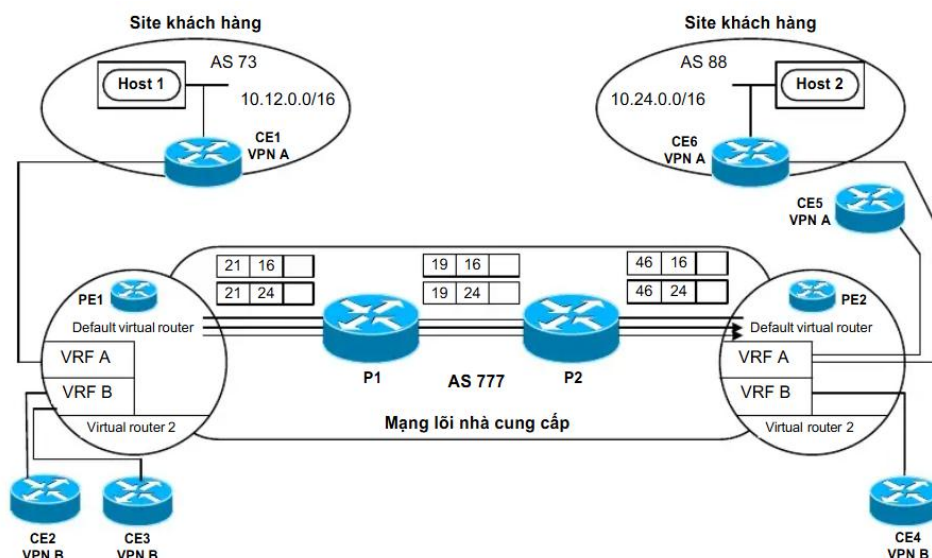


Hình 34 Cấu trúc gói dữ liệu L2TP

2.3.4 Mạng riêng ảo trên nền MPLS

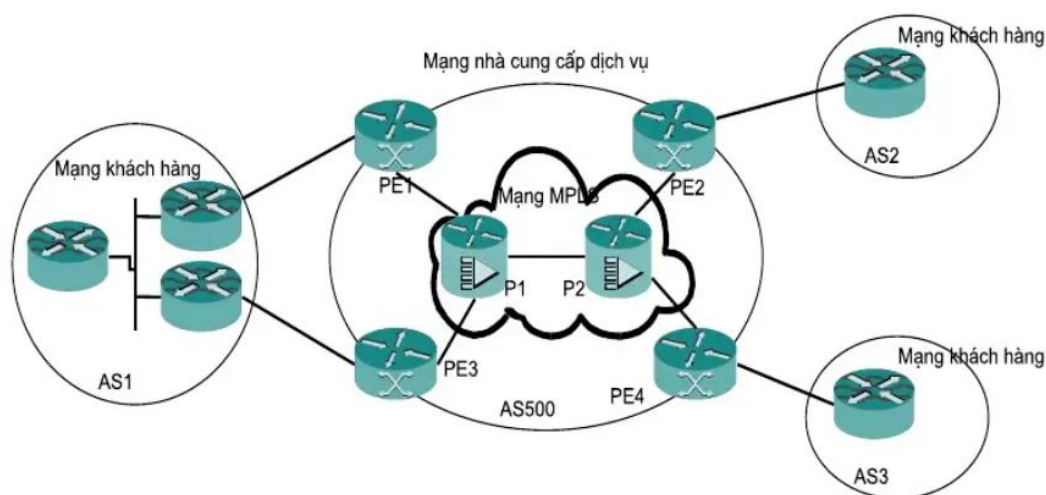
MPLS là một giao thức để tăng tốc và định hình luồng lưu lượng mạng. Đây là công nghệ chuyển mạch dựa trên nhãn được thiết kế để chuyển tiếp các gói tin hiệu quả hơn so với định tuyến truyền thống. MPLS hoạt động bằng cách gán nhãn cho các gói dữ liệu, sau đó được sử dụng để chuyển tiếp các quyết định trong mạng.

MPLS VPN, viết tắt của Multiprotocol Label Switching Virtual Private Network, bao gồm một tập hợp các kỹ thuật tận dụng Multiprotocol Label Switching (MPLS) để thiết lập mạng riêng ảo (VPN). Phương pháp này cung cấp tính linh hoạt đáng kể cho việc truyền và định tuyến lưu lượng mạng đa dạng bằng cách khai thác khả năng của xương sống MPLS.



Hình 35 Hoạt động chuyển tiếp dữ liệu VPN qua mạng MPLS

Mô hình MPLS VPN giống với mô hình router PE dành riêng (dedicated PE router model) trong các dạng thực thi VPN ngang cấp peer-to-peer VPN. Tuy nhiên, thay vì triển khai các router PE khác nhau cho từng khách hàng, lưu lượng khách hàng được tách riêng trên cùng router PE nhằm cung cấp khả năng kết nối vào mạng của nhà cung cấp cho nhiều khách hàng. Các thành phần của một MPLS VPN được trình bày trong hình sau:



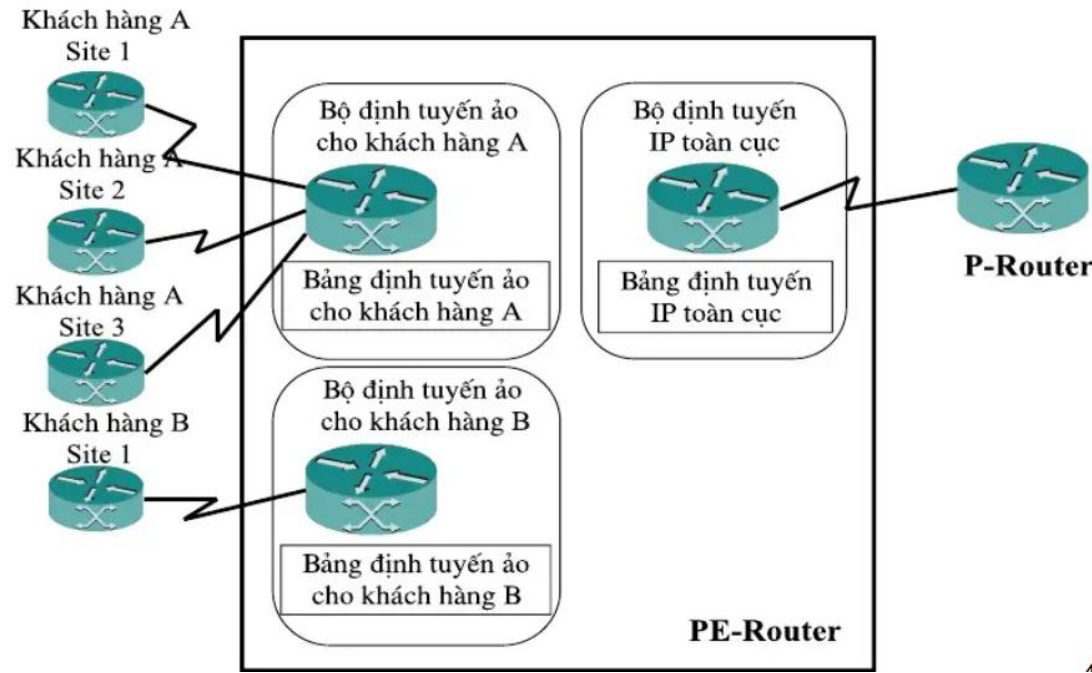
Hình 36 Các thành phần cơ bản của MPLS-VPN

- Mạng khách hàng – thường là miền điều khiển của khách hàng gồm các thiết bị hay các router trải rộng trên nhiều site của cùng một khách hàng. Các router CE – là những router trong mạng khách hàng giao tiếp với mạng của nhà cung cấp.
- Mạng của nhà cung cấp – miền thuộc điều khiển của nhà cung cấp gồm các router biên (edge) và lõi (core) để kết nối các site thuộc vào các khách hàng trong một hạ tầng mạng chia sẻ.

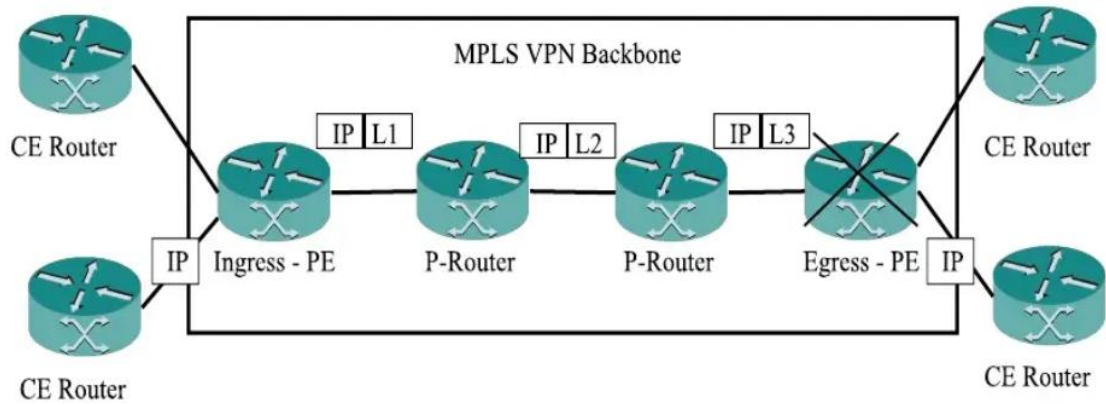
Mô hình định tuyến MPLS VPN:

- MPLS VPN giống như mô hình mạng ngang cấp với router dành riêng. Từ một router CE, chỉ cập nhật IPv4, dữ liệu được chuyển tiếp đến router PE. CE không cần bất kỳ một cấu hình riêng biệt nào cho phép nó tham gia vào miền MPLS VPN. Yêu cầu duy nhất trên CE là một giao thức định tuyến (hay tuyến tĩnh(static)/tuyến ngầm định (default)) cho phép nó trao đổi thông tin định tuyến IPv4 với các router PE.
- Trong mô hình MPLS VPN, router PE thực hiện rất nhiều chức năng. Trước tiên nó phải phân tách lưu lượng khách hàng nếu có nhiều hơn một khách hàng kết nối tới nó. Vì thế, mỗi khách hàng được gán với một bảng định tuyến độc

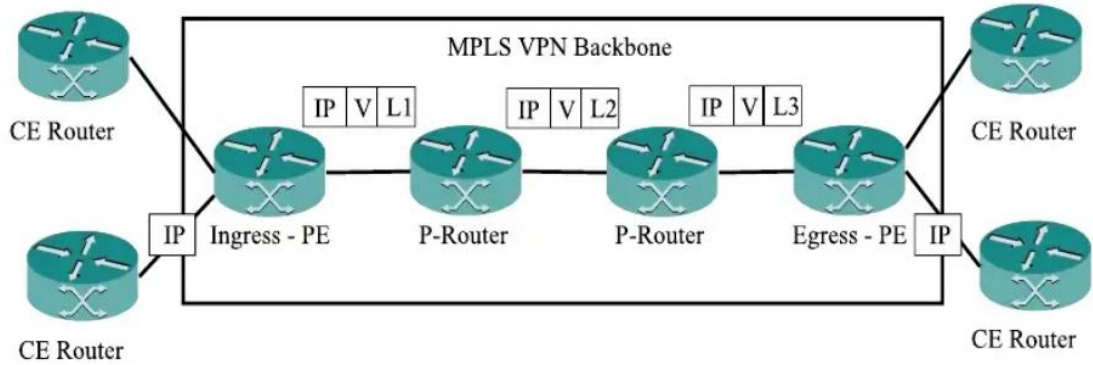
lập. Định tuyến qua SP backbone thực hiện bằng một tiến trình định tuyến trong bảng định tuyến toàn cục.



Hình 37 Bộ định tuyến PE và sơ đồ kết nối các site khách hàng



Hình 38 Sử dụng nhãn để chuyển tiếp gói tin VPN



Hình 39 Sử dụng ngăn xếp nhãn để chuyển tiếp gói tin VPN

2.3.5 So sánh MPLS-VPN với IPSec-VPN

Đặc điểm	MPLS-VPN	IPSec-VPN
Cấu hình	Điểm tới điểm, Hub-and-Spoke, cấu hình đầy đủ	Điểm tới điểm, Hub-and-Spoke, cấu hình đầy đủ
Bảo mật / Xác thực phiên	Thiết lập các thành viên VPN trong quá trình cung cấp dịch vụ, định nghĩa truy nhập tới nhóm dịch vụ trong khi cấu hình, từ chối các truy nhập không hợp pháp.	Xác thực qua chứng thực số hoặc khóa xác định trước. Loại bỏ gói không phù hợp với chính sách bảo mật.
Tính riêng tư	Tách lưu lượng thành các luồng riêng biệt	Sử dụng mã hoá và kỹ thuật đường hầm thích hợp tại lớp địa chỉ mạng.
QoS và SLA	Cho phép lập các SLA với nhiều mức, có các kỹ thuật đảm bảo QoS và kỹ thuật lưu lượng.	Không chỉ ra các QoS và SLA trực tiếp.
Khả năng mở rộng	Có khả năng mở rộng cao vì không yêu cầu cấu hình đầy đủ hoặc ngang hàng.	Chấp nhận mở rộng theo kiểu Hub-and-Spoke. Khả năng mở rộng kéo theo các thách thức về kế hoạch, phân phối khóa, quản lý khóa và cấu hình các thiết bị bị ngang hàng.
Hỗ trợ điểm-điểm	Có.	Có.
Hỗ trợ truy nhập từ xa	Có nếu được kết nối với IPSec.	Có.
Cung cấp dịch vụ	Cần một lần cung cấp các thiết bị khách hàng và thiết bị biên mạng nhà cung cấp.	Giảm các chi phí điều hành mạng qua phương pháp cung cấp tập trung.
Triển khai dịch vụ	Yêu cầu các phần tử mạng MPLS mở dịch vụ tại các thiết bị lõi và biên của mạng nhà cung cấp.	Có thể triển khai trên bất kỳ hạ tầng mạng IP có sẵn.

Phần mềm Client VPN	Không yêu cầu, người sử dụng không cần phần mềm tương tác với mạng.	Cần phải có để khởi tạo các phần mềm chức năng.
---------------------	---------------------------------------------------------------------	-------------------------------------------------

Bảng 1. Bảng so sánh MPLS-VPN với IPSec-VPN

Việc mở rộng tiền tố địa chỉ IP của khách hàng VPN đã dẫn đến sự ra đời của khái niệm mới – địa chỉ VPN-IP (VPN-IPv4).

Địa chỉ VPN-IP được hình thành bằng cách kết hợp hai thành phần có độ dài cố định:

- Trường phân biệt tuyến (Route Distinguisher – RD) – 64 bit
- Địa chỉ IP cơ sở – 32 bit

Tổng cộng: 96 bit, đại diện cho địa chỉ VPNv4 duy nhất trong mạng MPLS.

Ý nghĩa: Việc bổ sung Route Distinguisher cho phép các khách hàng VPN sử dụng cùng một địa chỉ IP nội bộ mà không bị trùng lặp khi truyền tải trên mạng MPLS của nhà cung cấp.

2.3.6 Ngoài ra, còn một số giao thức phổ biến khác

2.3.6.1 SSL và TLS

Cả SSL và TLS đều sử dụng mật khẩu tương tự như IPSec để có thể bảo mật và chế độ Handshake nằm trong quá trình tải khoản client với server. Các khóa xác thực được lưu tại client và server sẽ là yếu tố tạo nên một kết nối thành công.

2.3.6.2 SSTP

Secure Socket Tunneling Protocol (SSTP) là sản phẩm VPN đến từ Microsoft và được sử dụng phổ biến trên hệ điều hành Windows. Trên phương diện lý thuyết, khi dùng với SSL, AES, SSTP sẽ cho ra hiệu năng bảo mật rất tốt. Hiện nay, bạn sẽ chưa dễ dàng tìm thấy các lỗi của dòng VPN được Microsoft lập trình. Tuy vậy, bạn sẽ mắc phải một vài điều khó khăn khi sử dụng trên những hệ điều hành khác Windows.

2.3.6.3 OpenVPN

OpenVPN được cung cấp đến thị trường vào năm 2001 và là bộ giao thức mở mang đến hiệu năng bảo mật đáng cân nhắc. Đối với khả năng mã hoá của OpenVPN thường dùng đến thư viện phần mềm bảo mật OpenSSL. Hiện tại, thư viện OpenSSL hỗ trợ lượng lớn thuật toán mã hoá khác nhau, trong đó AES là giao thức bảo mật nổi bật hàng đầu. Đối với hệ điều hành theo từng cấp, OpenVPN sẽ không có sự hỗ trợ.

2.3.6.4 SoftEther

So với những sản phẩm trước đó thì Software Ethernet được xuất hiện khá muộn vào năm 2014. Tương tự như OpenVPN, sản phẩm bảo mật này cũng sử dụng mã nguồn mở. Hiện nay, các giao thức mã hoá của SoftEther được xem là mạnh mẽ vượt trội gồm: RSA 4096-bit, AES-256. SoftEther có thể được cài đặt trên những hệ điều hành riêng lẻ bao gồm: IOS, MacOS, Android, Windows, Linux và Unix.

2.3.7 Cách chọn giao thức phù hợp

Trên thực tế, nhu cầu sử dụng mạng riêng ảo của người dùng là nhằm hạn chế bị lộ dữ liệu. Để chọn được một giao thức phù hợp, bạn nên chú trọng vào khả năng bảo mật của chúng. Qua các phân phân tích về những giao thức bảo mật tốt mà Vietnix là đề ra, bạn có thể dễ dàng nhận thấy được 3 cái tên sáng giá gồm: IKEv2, OpenVPN và SoftEther.

Trong đó cả OpenVPN và SoftEther đều có ưu điểm về mã nguồn mở, riêng IKEv2 sẽ có 2 hướng triển khai là mã nguồn mở và độc quyền. Đa phần người dùng sẽ lựa chọn OpenVPN hoặc IKEv2 vì đã có thời gian thẩm định và kiểm tra mức độ an toàn bảo mật. Đối với SoftEther chưa được dùng phổ biến nhưng cũng là cái tên đáng cân nhắc để trải nghiệm.

2.4 Kết chương

Chương 2 đã trình bày chi tiết kiến trúc hệ thống VPN và các giao thức chính như IPSec, PPTP, L2TP, SSL/TLS... Những phân tích kỹ thuật giúp người học hiểu được cách các giao thức hoạt động và chọn lựa phù hợp với từng mục tiêu bảo mật cụ thể.

CHƯƠNG 3. : CÁC VẤN ĐỀ AN NINH CỦA VPN

3.1 Hệ thống phát hiện xâm nhập dựa trên khai phá dữ liệu trong VPN

Để giải quyết vấn đề công nghệ truyền thống không thể đáp ứng đầy đủ yêu cầu về bảo mật thông tin trong VPN, Bằng cách nghiên cứu nguyên lý hoạt động của VPN, đưa ra một giải pháp tích hợp hệ thống phát hiện xâm nhập vào VPN. Thuật toán khai phá dữ liệu dựa trên luật kết hợp được áp dụng để phát hiện hành vi tấn công. Kết quả thực nghiệm cho thấy mô hình giúp tăng hệ số tin cậy của người dùng lên 60% so với mạng truyền thống, là một biện pháp bảo vệ hiệu quả, giúp giảm thiểu hoặc ngăn chặn tổn thất do các cuộc tấn công mạng gây ra.

3.1.1 Giới thiệu

Internet ngày càng đóng vai trò không thể thiếu trong cuộc sống hàng ngày. Tuy nhiên, sự xuất hiện của các loại virus mạng và tin tặc đã gây ra nhiều bất tiện và tổn thất cho người dùng, ví dụ như: tê liệt máy chủ, đánh cắp dữ liệu nội bộ. Những vấn đề này càng trở nên nghiêm trọng hơn đối với người dùng VPN.

Theo thống kê từ nhóm phản ứng sự cố máy tính CERT/CC (Hoa Kỳ), số lượng sự kiện tấn công mạng đang tăng theo cấp số nhân mỗi năm. Do đó, cần có phương pháp xác định và kiểm soát hiệu quả các cuộc tấn công mạng, từ đó giảm thiểu thiệt hại do virus gây ra.

Mặc dù đã có nhiều công nghệ bảo mật được phát triển như xác thực, kiểm soát truy cập, tường lửa, định tuyến an toàn, mã hóa..., nhưng tin tặc cũng không ngừng nâng cấp kỹ thuật tấn công. Do đó, việc phát hiện xâm nhập trở thành mắt xích quan trọng trong bảo đảm an toàn thông tin, khắc phục được những điểm yếu của công nghệ bảo mật truyền thống.

3.1.2 Tổng quan về hệ thống phát hiện xâm nhập (IDS)

Hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) về mặt bề ngoài giống như thiết bị giám sát mạng và cảnh báo, có khả năng quan sát, phân tích các cuộc tấn công mạng, gửi cảnh báo sớm và thực hiện các biện pháp phản ứng nhằm giảm thiểu tổn thất.

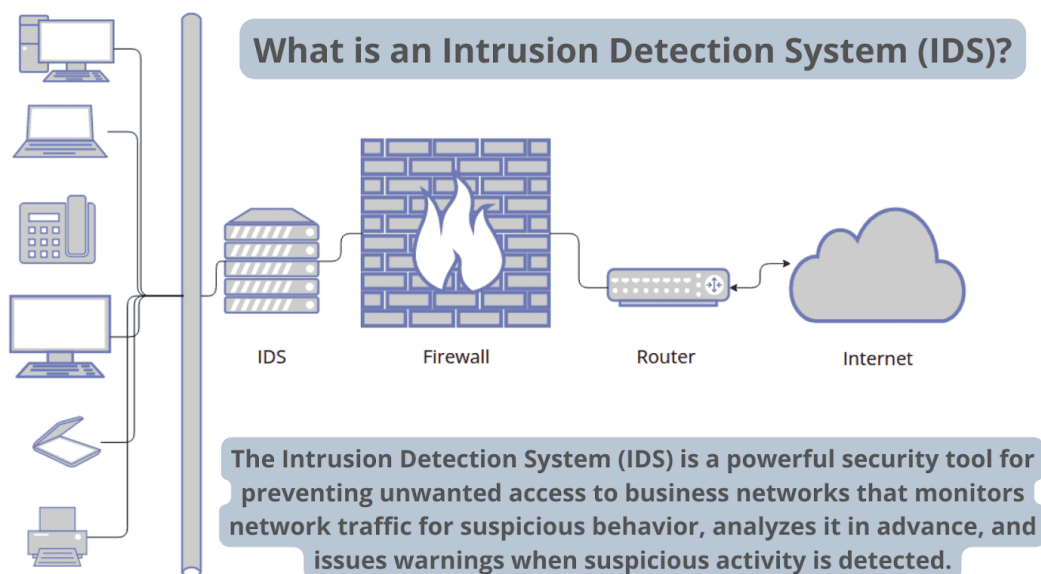
IDS giúp phát hiện các hành vi cố tình phá hoại tính toàn vẹn, tính xác thực và tính sẵn sàng của tài nguyên máy tính. Nó giám sát hoạt động hệ thống theo thời gian thực, phát hiện các hành vi tấn công và đưa ra biện pháp thích hợp.

Hai tiêu chí chính để đánh giá hệ thống IDS:

- Tỷ lệ phát hiện (Detection Rate) – càng cao càng tốt
- Tỷ lệ báo động sai (False Alarm Rate) – càng thấp càng tốt

Vì IDS phân tích hành vi người dùng dưới dạng dữ liệu, nên vấn đề cốt lõi là: xử lý dữ liệu thu thập được sao cho đúng và hiệu quả để đưa ra kết luận chính xác.

3.1.3 Cấu trúc hệ thống IDS



Hình 40 Sơ đồ mô tả chức năng của hệ thống phát hiện xâm nhập

Theo chức năng, hệ thống IDS gồm các thành phần:

- Bộ thu thập và phát hiện dữ liệu mạng
- Kho mẫu tấn công
- Cảnh báo và phản ứng
- Công bố thông tin phát hiện

3.1.4 Hệ thống phát hiện xâm nhập dựa trên khai phá dữ liệu

3.1.4.1 Khai phá dữ liệu

Khai phá dữ liệu là quá trình trích xuất các mẫu mô tả từ tập dữ liệu lớn. Khai phá luật kết hợp nhằm tìm ra mối liên hệ giữa các đặc trưng trong dữ liệu.

Luật kết hợp được biểu diễn dưới dạng:

$X \rightarrow Y$, với các chỉ số: Support và Confidence.

Thuật toán phổ biến là Apriori, cho phép tìm ra các tập mục phổ biến, các luật liên kết có ý nghĩa giữa các tập mục.

3.1.4.2 Thuật toán Apriori

Thuật toán Apriori hoạt động như sau:

- Duyệt từng giao dịch $t \rightarrow$ đếm số lượng tập mục

- Sinh các tập mục ứng viên
- Đếm số lượng xuất hiện
- Lọc các tập mục không phổ biến (không đạt ngưỡng support)
- Trả về tập mục phổ biến

Các bước xử lý gồm:

- Sinh ứng viên từ tập mục phổ biến (k-1)
- Duyệt từng cặp để ghép thành ứng viên cấp k
- Loại bỏ các tập có tập con không phổ biến

3.1.4.3 Mô hình phát hiện xâm nhập dựa trên khai phá dữ liệu

Hệ thống IDS sẽ:

1. Thu thập dữ liệu: từ máy chủ hoặc mạng.
2. Tiền xử lý dữ liệu: lọc, định dạng, chuẩn hóa.
3. Khai phá dữ liệu: sử dụng luật kết hợp, phân cụm, phân loại.
4. Phát hiện xâm nhập: so sánh mẫu thu được với cơ sở tri thức.

Luồng hoạt động:

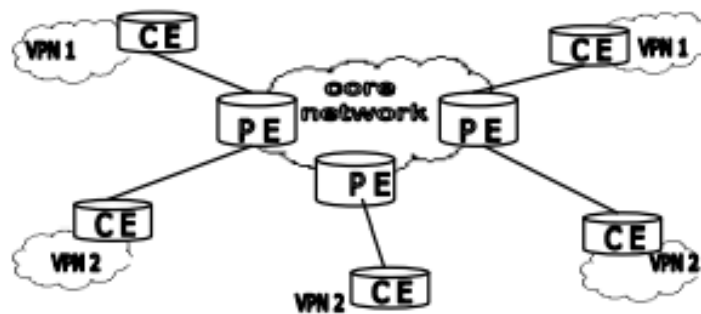
- Dữ liệu gốc → xử lý → tạo tập dữ liệu xử lý
- Áp dụng luật khai phá để trích xuất đặc trưng → lưu vào kho tri thức
- Dữ liệu mới được so sánh với kho tri thức để xác định có xâm nhập hay không
- Kết quả (xâm nhập hay không) được báo cáo cho quản trị viên

Nếu phát hiện hành vi bất thường, hệ thống sẽ cảnh báo cho quản trị viên và cập nhật kho luật.

3.1.5 Hệ thống phát hiện xâm nhập trong ứng dụng VPN

VPN truyền dữ liệu giữa hai mạng thông qua đường hầm trong mạng diện rộng (WAN). Mặc dù đã có áp dụng kỹ thuật mã hóa, nhưng vẫn chưa đáp ứng được yêu cầu bảo mật của các doanh nghiệp lớn.

Do đó, cần tích hợp IDS vào môi trường VPN để cung cấp cấp độ bảo mật cao hơn. IDS sẽ giám sát các dữ liệu truyền qua đường hầm VPN, phát hiện các hành vi xâm nhập không mong muốn.



Hình 41 Hệ thống phát hiện xâm nhập trong ứng dụng VPN

3.2 Mạng VPN liên nhà cung cấp sử dụng phương pháp VRF Back-to-Back và MP-eBGP

Công nghệ MPLS đang được nhiều nhà cung cấp dịch vụ trên toàn cầu áp dụng để kết nối các vị trí khách hàng phân tán về địa lý. Phương pháp thiết kế mạng VPN liên nhà cung cấp (Inter-provider VPN), nơi các chi nhánh hoặc đối tác của một tổ chức nằm ở các khu vực không cùng ISP. Hai phương pháp chính được nghiên cứu là:

- Back-to-Back VRF: Mỗi nhà cung cấp dịch vụ cấu hình VRF riêng biệt và kết nối qua các giao diện vật lý.
- MP-eBGP giữa ASBR: Dùng BGP để trao đổi thông tin định tuyến giữa các nhà cung cấp mà không cần cấu hình VRF riêng biệt trên từng ASBR.

3.2.1 Giới thiệu

Một công ty với nhiều chi nhánh có thể lựa chọn kết nối qua đường thuê riêng, frame relay hoặc MPLS. Ngoài ra, họ có thể kết nối qua Internet công cộng nhưng sẽ đối mặt với rủi ro bảo mật. Do đó, giải pháp VPN liên nhà cung cấp với IP riêng và công nghệ MPLS ra đời nhằm đảm bảo bảo mật và hiệu suất.

3.2.2 Mạng riêng ảo VPN

VPN (Virtual Private Network – Mạng riêng ảo) là một mạng sử dụng các tuyến đường công cộng nhưng vẫn duy trì tính bảo mật và bảo vệ đối với các mạng riêng. VPN cho phép tạo kết nối an toàn tới một mạng khác thông qua Internet.

Đây là hệ thống hiện có nhằm tạo kết nối bảo mật thông qua các kết nối dựa trên địa chỉ IP công cộng. Khi chúng ta duyệt web với tư cách người dùng VPN, máy tính của chúng ta sẽ liên lạc với website thông qua kết nối được mã hóa của VPN. VPN sẽ chuyển tiếp yêu cầu tới trang web và sau đó gửi lại phản hồi từ trang web qua kết nối an toàn.

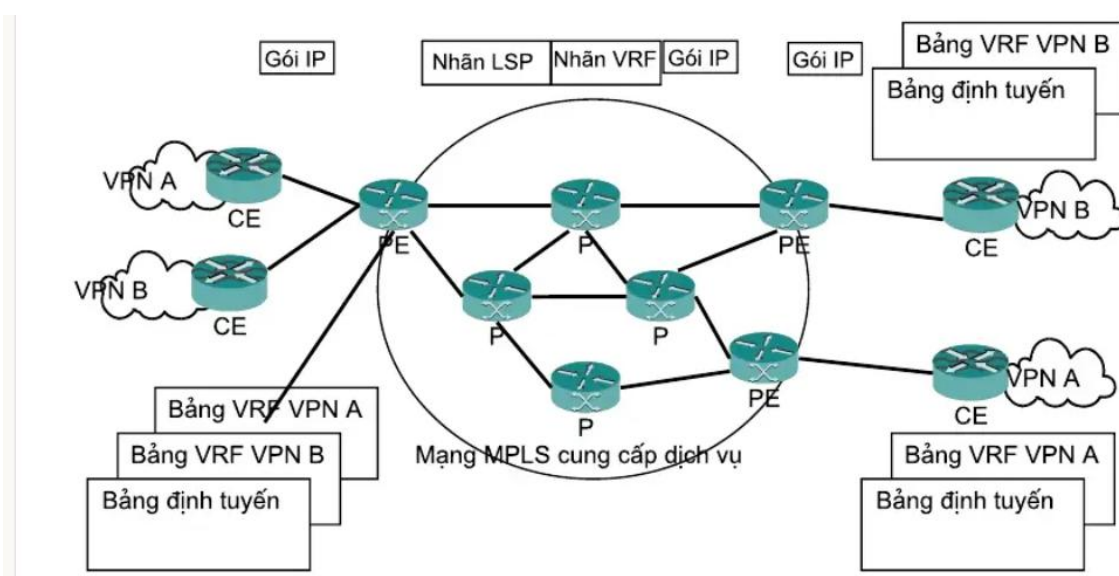
Ví dụ: nếu chúng ta sử dụng VPN có máy chủ đặt tại Mỹ để truy cập iTunes, thì iTunes sẽ nhận thấy kết nối của chúng ta đến từ Mỹ. Từ "ảo" (virtual) ở đây

ám chỉ việc dữ liệu không được truyền vật lý trực tiếp, mà là được ghép kênh logic từ nhiều VPN khác nhau.

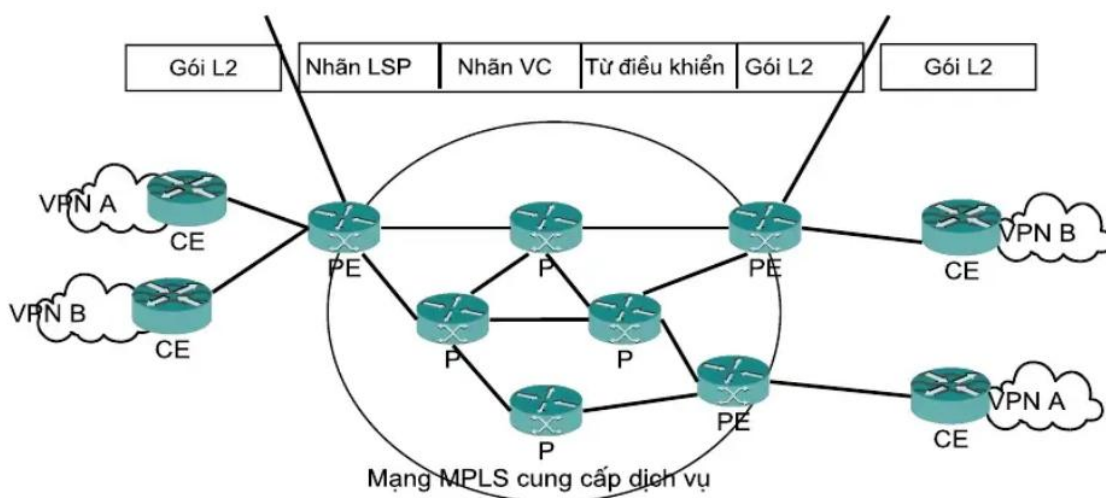
Một số tính năng quan trọng của VPN bao gồm:

- Bảo mật (Confidentiality)
- Chống phát lại (Anti-replay)
- Xác thực (Authentication)
- Tính toàn vẹn (Integrity)

VPN có thể hoạt động ở nhiều tầng trong mô hình mạng, chẳng hạn như VPN tầng 2 (L2VPN) và VPN tầng 3 (L3VPN), với các tiêu chuẩn và yêu cầu bảo mật khác nhau.



Hình 42 Mô hình MPLS L3VPN



Hình 43 Mô hình MPLS L2VPN

VPN bảo mật là lựa chọn tốt nhất để tăng cường bảo mật trong truyền thông IP hiện nay. So với SSL VPN, IPSec VPN có khả năng bảo vệ toàn bộ lưu lượng ở tầng mạng, bảo vệ được cả tiêu đề IP và dữ liệu, từ đó chống lại được nhiều dạng tấn công mạng hơn.

3.2.3 Công nghệ MPLS và VPN

MPLS là viết tắt của Multiprotocol Label Switching – một cơ chế truyền tải dữ liệu ở tầng 2.5 trong mô hình OSI, tức nằm giữa tầng liên kết dữ liệu (Data Link Layer) và tầng mạng (Network Layer).

MPLS sử dụng các nhãn (label) để định tuyến gói tin, thay vì sử dụng thông tin định tuyến IP truyền thống. Khi một gói tin đi vào mạng MPLS, một nhãn sẽ được gán vào gói tin đó dựa trên bảng định tuyến tại thiết bị đầu vào. Các bộ định tuyến trung gian sau đó chỉ cần dựa vào nhãn thay vì địa chỉ IP để tiếp tục chuyển tiếp gói tin – từ đó giúp tăng tốc độ xử lý và nâng cao hiệu suất mạng.

MPLS VPN là công nghệ ứng dụng MPLS trong xây dựng mạng riêng ảo, cho phép kết nối các site khách hàng qua mạng backbone của nhà cung cấp dịch vụ. Các mạng của khách hàng (Customer Edge - CE) kết nối tới bộ định tuyến PE (Provider Edge) của nhà cung cấp dịch vụ. Mỗi site được gán một bảng định tuyến riêng (VRF – Virtual Routing and Forwarding), cho phép nhiều khách hàng dùng cùng một địa chỉ IP mà không bị xung đột.

MPLS VPN cung cấp:

- Định tuyến cách ly giữa các khách hàng
- Bảo mật nhờ mô hình mạng riêng
- Hiệu suất cao do sử dụng định tuyến nhãn
- Hỗ trợ nhiều dịch vụ giá trị gia tăng

Tại Ấn Độ, các nhà cung cấp dịch vụ như BSNL, Airtel, Reliance... đều đang cung cấp dịch vụ MPLS VPN cho khách hàng doanh nghiệp. Các gói dịch vụ thường dựa trên yêu cầu cụ thể của doanh nghiệp về băng thông, phạm vi kết nối, mức độ bảo mật và quản lý.

Chi phí triển khai MPLS VPN dao động từ 5 đến 7 lakh INR/năm cho một tổ chức, tùy thuộc vào quy mô, mức độ ưu tiên dữ liệu và các tính năng bổ sung.

3.2.4 Thách thức của VPN Internet

VPN sử dụng Internet làm phương tiện truyền dẫn có thể bị tấn công: IP spoofing, phishing, ransomware, DDoS, v.v. Các rủi ro này ảnh hưởng nghiêm

trọng đến doanh nghiệp, đặc biệt là các tổ chức nhỏ không có hệ thống bảo mật tốt.

3.2.5 Mạng VPN liên nhà cung cấp (Inter-Provider VPN)

Trong môi trường mạng hiện đại, các doanh nghiệp thường có các chi nhánh phân bố tại nhiều khu vực địa lý khác nhau và có thể sử dụng các nhà cung cấp dịch vụ Internet (ISP) khác nhau. Để đảm bảo kết nối an toàn và hiệu quả giữa các chi nhánh này, việc triển khai mạng riêng ảo liên nhà cung cấp (Inter-provider VPN) trở nên cần thiết.

3.2.5.1 Phương pháp VRF nối tiếp (Back-to-Back VRF)

Phương pháp này yêu cầu mỗi nhà cung cấp dịch vụ cấu hình bảng định tuyến và chuyển tiếp ảo (VRF) riêng cho từng khách hàng. Các VRF này sau đó được kết nối trực tiếp với nhau thông qua các giao diện vật lý hoặc logic. Mỗi VRF được cấu hình với các giao thức định tuyến như eBGP, OSPF, EIGRP hoặc định tuyến tĩnh để trao đổi thông tin định tuyến với VRF tương ứng ở phía nhà cung cấp dịch vụ khác.

Ưu điểm:

- **Đơn giản trong triển khai:** Dễ dàng cấu hình và triển khai, phù hợp với các môi trường mạng nhỏ hoặc khi chỉ có một số ít khách hàng cần kết nối liên nhà cung cấp.
- **Bảo mật cao:** Do không có sự chia sẻ thông tin định tuyến giữa các nhà cung cấp dịch vụ, mức độ bảo mật được tăng cường.

Nhược điểm:

- **Khả năng mở rộng hạn chế:** Mỗi khách hàng yêu cầu một VRF riêng biệt trên cả hai nhà cung cấp dịch vụ, dẫn đến việc quản lý phức tạp khi số lượng khách hàng tăng lên.
- **Yêu cầu nhiều tài nguyên:** Việc duy trì nhiều VRF và phiên định tuyến riêng biệt tiêu tốn nhiều tài nguyên hệ thống.

3.2.5.2 Phương pháp MP-eBGP giữa các ASBR

Phương pháp này sử dụng Multiprotocol External BGP (MP-eBGP) để trao đổi thông tin định tuyến VPNv4 giữa các bộ định tuyến biên của hệ thống tự trị (ASBR) thuộc các nhà cung cấp dịch vụ khác nhau. MP-eBGP cho phép truyền tải các tuyến đường VPNv4 cùng với các nhãn MPLS, giúp duy trì thông tin định tuyến và nhãn xuyên suốt giữa các nhà cung cấp dịch vụ.

Ưu điểm:

- **Khả năng mở rộng tốt:** Không cần cấu hình VRF trên các ASBR, giảm thiểu số lượng cấu hình cần thiết và đơn giản hóa quản lý.
- **Hiệu quả trong phân phối nhãn:** Nhãn MPLS được phân phối cùng với thông tin định tuyến, giúp duy trì tính toàn vẹn của đường dẫn VPN.

Nhược điểm:

- **Phức tạp trong triển khai:** Yêu cầu hiểu biết sâu về MP-eBGP và cách thức hoạt động của MPLS VPN.
- **Phụ thuộc vào sự hợp tác giữa các nhà cung cấp dịch vụ:** Cần có sự phối hợp chặt chẽ giữa các nhà cung cấp dịch vụ để đảm bảo hoạt động trơn tru của mạng VPN liên nhà cung cấp.

3.2.6 Kết quả mô phỏng

Để kiểm tra và xác minh hoạt động của mạng VPN liên nhà cung cấp, sử dụng phần mềm mô phỏng mạng GNS3 để thiết lập và kiểm tra các cấu hình như sau:

3.2.6.1 Mô hình mạng

Mô hình mạng bao gồm hai nhà cung cấp dịch vụ (ISP A và ISP B), mỗi ISP có một bộ định tuyến biên nhà cung cấp (PE). Các bộ định tuyến biên hệ thống tự trị (ASBR) được sử dụng để kết nối giữa hai ISP. Các thiết bị đầu cuối của khách hàng (CE) được kết nối với các PE tương ứng.

3.2.6.2 Cấu hình định tuyến

1. Định tuyến nội bộ (IGP): Sử dụng giao thức OSPF để thiết lập định tuyến nội bộ trong mỗi ISP.

2. Định tuyến giữa các ISP:

- **Phương pháp VRF nối tiếp (Back-to-Back VRF):** Mỗi ASBR được cấu hình với các VRF tương ứng và kết nối với nhau thông qua các giao diện vật lý hoặc logic.
 - **Phương pháp MP-eBGP giữa các ASBR:** Sử dụng Multiprotocol External BGP (MP-eBGP) để trao đổi thông tin định tuyến VPNv4 giữa các ASBR.
3. Cấu hình MPLS: MPLS được kích hoạt trên các giao diện giữa PE và ASBR để hỗ trợ chuyển tiếp gói tin dựa trên nhãn.

3.2.6.3 Kiểm tra kết nối

Sau khi hoàn tất cấu hình, thực hiện các kiểm tra sau:

- Kiểm tra kết nối giữa các CE: Sử dụng lệnh ping từ CE1 (thuộc ISP A) đến CE2 (thuộc ISP B) để xác minh kết nối xuyên qua mạng liên nhà cung cấp.

- Kiểm tra bảng định tuyến: Sử dụng lệnh show ip route và show ip bgp vpnv4 trên các PE và ASBR để xác minh việc trao đổi thông tin định tuyến VPNv4.Cisco
- Kiểm tra nhãn MPLS: Sử dụng lệnh show mpls forwarding-table để xác minh việc gán và chuyển tiếp nhãn MPLS.

3.2.6.4 Kết quả

Kết quả kiểm tra cho thấy:

- Các CE có thể giao tiếp với nhau thông qua mạng liên nhà cung cấp mà không gặp sự cố.
- Thông tin định tuyến VPNv4 được trao đổi chính xác giữa các PE và ASBR.
- Nhãn MPLS được gán và chuyển tiếp đúng cách, đảm bảo hiệu suất và bảo mật của mạng.

3.3 Phân tích VPN và Góc nhìn Mới để Bảo vệ Mạng Thoại qua VPN

Bảo mật và quyền riêng tư đang trở thành yêu cầu bắt buộc đối với truyền thông VoIP. Những yêu cầu này bao gồm: tính bảo mật, toàn vẹn, xác thực, chống phát lại và chống chối bỏ. Các giải pháp hiện có thường mang tính tổng quát và không xét đến các đặc thù riêng của thoại, dẫn đến ảnh hưởng đến QoS do trễ, jitter và mất gói.

Do đó, cần có các giải pháp bảo mật mới đáp ứng ràng buộc thời gian thực, xử lý được các loại tấn công và hạn chế được chi phí tính toán. VPN hiện là một trong những giải pháp mạnh nhất cho truyền thông qua mạng IP, nhưng lại chưa đáp ứng tốt việc xử lý thoại thời gian thực.

3.3.1 Giới thiệu

VoIP là một trong những ứng dụng Internet phát triển nhanh nhất, nhưng bảo vệ nó lại là vấn đề lớn vì:

- Bảo mật thường đi ngược lại hiệu suất
- Việc thêm lớp bảo mật ảnh hưởng đến QoS của thoại

Các yêu cầu bảo mật bao gồm:

- Xác thực (authentication)
- Bảo mật và riêng tư (confidentiality, privacy)
- Toàn vẹn (integrity)
- Chống chối bỏ (non-repudiation)
- Chống phát lại (non-replay)

- Khả dụng tài nguyên (resource availability)

VPN là giải pháp bảo mật mạnh cho truyền thông giữa người dùng với mạng nội bộ qua Internet. VPN có 2 thành phần:

- Dịch vụ bảo mật
- Đường hầm truyền dữ liệu riêng tư

VPN sử dụng mã hóa để chống nghe lén và phân tích gói trên mạng công cộng. Có 3 loại VPN:

- Remote Access VPN (User ↔ LAN)
- Site-to-site VPN (Chi nhánh ↔ Trụ sở)
- Extranet VPN (Doanh nghiệp ↔ Đối tác)

Tuy nhiên, VPN ảnh hưởng tới chất lượng thoại (latency, jitter, loss), vì thế cần nghiên cứu giải pháp tối ưu.

3.3.2 Giao thức VPN (VPN Protocols)

Giao thức VPN có thể được triển khai ở nhiều tầng trong mô hình OSI:

- Tầng liên kết dữ liệu (Data Link Layer)
- Tầng mạng (Network Layer)
- Tầng phiên (Session Layer)

Dưới đây là mô tả các giao thức tương ứng tại các tầng:

3.3.2.1 Tầng liên kết dữ liệu – VPN tầng 2 (L2 VPN)

PTP (Point to Point Tunneling Protocol)

- Là giao thức VPN cũ, đơn giản, dễ triển khai
- Hạn chế về bảo mật (sử dụng MS-CHAP dễ bị tấn công)
- Hỗ trợ đa nền tảng nhưng yếu kém về mã hóa và xác thực

L2TP (Layer 2 Tunneling Protocol)

- Kết hợp giữa PPTP và L2F
- Không cung cấp mã hóa – phải kết hợp với IPSec để bảo mật
- Có thể hoạt động qua nhiều loại mạng, nhưng cấu hình phức tạp

3.3.2.2 Tầng mạng – VPN tầng 3 (L3 VPN)

IPSec (Internet Protocol Security)

- Mạnh nhất về bảo mật, hoạt động ở tầng IP
- Cung cấp: xác thực, toàn vẹn, bảo mật và chống phát lại

Có 2 chế độ:

- **Transport mode:** chỉ mã hóa payload
- **Tunnel mode:** mã hóa toàn bộ gói IP (IP header + payload)

Hai giao thức chính:

- AH (Authentication Header) – xác thực, không mã hóa
- ESP (Encapsulating Security Payload) – mã hóa và xác thực

IPSec dùng phân biệt giao thức dựa vào:

- Chỉ số tham chiếu bảo mật SPI (Security Parameter Index)
- IP đích
- Giao thức AH hoặc ESP

IPSec hỗ trợ xác thực thông qua:

- Khóa chia sẻ trước (Pre-shared key)
- Chứng chỉ số (Certificate)
- Xác thực RSA

3.3.2.3 Tầng phiên – VPN ứng dụng (SSL/TLS VPN)

SSL VPN (Secure Socket Layer VPN)

- Dễ triển khai, hoạt động qua trình duyệt
- Không yêu cầu cài đặt phần mềm riêng trên máy khách
- Chỉ mã hóa payload – không mã hóa IP header
- Phù hợp cho người dùng di động

SSL VPN sử dụng:

- Xác thực người dùng
- Chứng chỉ máy chủ
- Giao tiếp được mã hóa (SSL/TLS)

3.3.2.4 So sánh các giao thức VPN

Tiêu chí	PPTP	L2TP	IPSec	SSL VPN
Bảo mật	Thấp	Trung bình	Cao	Cao
Mã hóa	RC4 yếu	Kết hợp IPSec	AES, 3DES	SSL/TLS
Cấu hình	Dễ	Phức tạp	Phức tạp	Dễ

Hỗ trợ đa nền tảng	Tốt	Tốt	Tốt	Rất tốt
Tầng hoạt động	L2	L2	L3	Session

Bảng 2. Bảng so sánh các giao thức VPN

3.3.3 Bảo mật thoại trên VPN (Voice over VPN Security)

3.3.3.1 Giới thiệu về bảo mật VoIP

VoIP (Voice over IP) đã trở nên phổ biến do tính linh hoạt và tiết kiệm chi phí. Tuy nhiên, khi truyền qua mạng IP công cộng, dữ liệu thoại dễ bị:

- Nghe trộm (eavesdropping)
- Giả mạo danh tính (spoofing)
- Tấn công từ chối dịch vụ (DoS/DDoS)
- Làm sai lệch dữ liệu (data tampering)

Mặc dù VPN cung cấp mã hóa và bảo vệ dữ liệu, nó chưa đủ hiệu quả cho thoại do ảnh hưởng đến hiệu suất và độ trễ.

3.3.3.2 Thách thức bảo mật trong Voice over VPN

Các vấn đề chính:

- Độ trễ cao (Latency):
 - VPN mã hóa và giải mã làm tăng thời gian xử lý
 - Mỗi gói thoại bị xử lý nặng hơn → ảnh hưởng trực tiếp đến trải nghiệm người dùng
- Mất gói (Packet loss):
 - VPN không cung cấp cơ chế chống mất gói
 - Gói thoại bị mất sẽ không được gửi lại, gây gián đoạn âm thanh
- Jitter (dao động độ trễ):
 - Khi độ trễ giữa các gói không đồng đều → giọng nói bị ngắt quãng
 - VPN không có cơ chế quản lý jitter riêng
- Chi phí tính toán cao:
 - VPN sử dụng thuật toán mã hóa mạnh như AES, 3DES...
 - Việc xử lý nặng làm giảm khả năng mở rộng khi có nhiều cuộc gọi đồng thời

3.3.3.3 Các yêu cầu bảo mật cụ thể với thoại qua VPN

Đối với VoIP chạy qua VPN, cần đáp ứng:

- **Xác thực đầu cuối (End-to-End Authentication):** Đảm bảo chỉ người dùng hợp lệ mới có thể tham gia cuộc gọi.
- **Bảo mật truyền dữ liệu (Data Confidentiality):** Nội dung thoại phải được mã hóa để tránh nghe lén.
- **Toàn vẹn dữ liệu (Integrity):** Bảo vệ khỏi sửa đổi gói tin trong quá trình truyền.
- **Chống phát lại (Anti-Replay):** Ngăn hacker ghi lại rồi phát lại gói tin để phá hoại hoặc đánh lừa hệ thống.
- **Chống chối bỏ (Non-Repudiation):** Bên gửi không thể phủ nhận đã gửi cuộc gọi hoặc dữ liệu.

Tuy nhiên, tất cả các cơ chế bảo mật trên phải nhẹ, nhanh và tương thích với thời gian thực – đó là thách thức lớn nhất khi triển khai VPN cho thoại.

3.3.4 Giải pháp bảo mật đề xuất (Proposed Security Solution)

3.3.4.1 Mục tiêu giải pháp

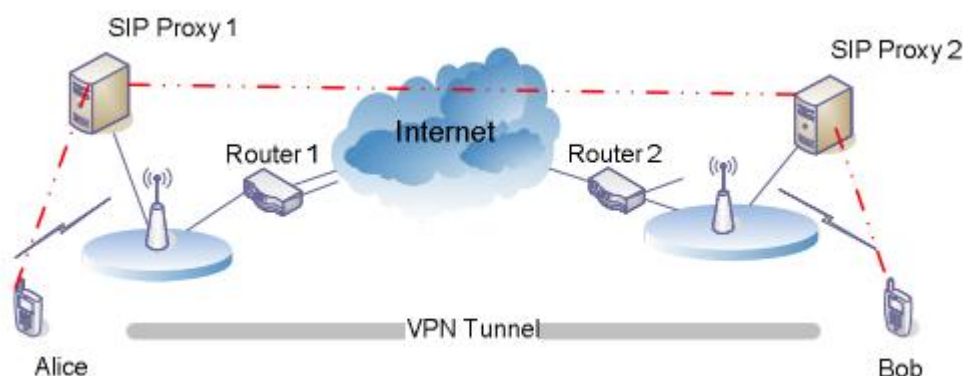
Mục tiêu là thiết kế một giải pháp VPN:

- Bảo vệ dữ liệu thoại
- Duy trì chất lượng dịch vụ (QoS)
- Hạn chế độ trễ, jitter và mất gói
- Giảm chi phí tính toán

3.3.4.2 Kiến trúc hệ thống

Thành phần chính bao gồm:

- VoIP clients (người dùng gọi)
- VPN Gateways (đầu vào và đầu ra bảo mật)
- VPN Tunnel (đường hầm bảo mật IPSec)
- Key Server (máy chủ quản lý khóa mã hóa)
- Policy Server (máy chủ kiểm soát chính sách bảo mật)



Hình 44 Mô hình kiến trúc bảo mật thoại qua VPN: Người dùng Alice và Bob kết nối qua đường hầm VPN bảo mật. Cuộc gọi thoại định tuyến qua các SIP Proxy và truyền qua Internet nhưng vẫn giữ được tính riêng tư nhờ cơ chế mã hóa VPN.

Giả định rằng Alice đang ở trong một mạng nội bộ (intranet) và muốn khởi tạo một cuộc gọi điện thoại qua Internet với Bob – người đang ở trong một intranet khác.

Các thiết bị đầu cuối của Alice và Bob (User Agent – UA) có thể là:

- Điện thoại SIP phần cứng, hoặc
- Phần mềm điện thoại (softphone) chạy trên máy tính.

Kiến trúc đề xuất sử dụng máy chủ SIP proxy trong mỗi intranet, với mục đích:

- Khởi tạo phiên kết nối (session initiation)
- Xác thực người dùng và thiết bị đầu cuối

Quy trình thiết lập cuộc gọi:

1. Alice gửi một thông điệp INVITE đến SIP Proxy Server 1 trong mạng nội bộ của cô ấy.

- Thông điệp INVITE được tạo bởi UA (User Agent) của Alice.
- Payload của INVITE gồm:
 - Mô tả phương tiện truyền thông (media description)
 - Thông điệp MIKEY cho IPSec (dùng để thương lượng khóa mã hóa)

2. SIP Proxy 1 chuyển tiếp thông điệp INVITE đến máy chủ chuyển hướng (redirect server).

- Redirect server sẽ truy xuất địa chỉ IP hiện tại của Bob để làm thông tin liên hệ.
- Từ đó, Proxy 1 có thể chuyển tiếp yêu cầu đến đúng người dùng (Bob).

3. Thay mặt Alice, SIP Proxy 1 thực hiện truy vấn DNS để xác định proxy server thuộc domain 2 (mạng của Bob), chuyển tiếp yêu cầu INVITE tới SIP Proxy 2.

4. SIP Proxy 2 sử dụng Location Server (thường là DNS) để tìm vị trí hiện tại của Bob.

- DNS trả lời rằng Bob đang đăng nhập ở domain 2.
- Thông tin này được biết nhờ cấu hình tĩnh được thiết lập trước bởi Bob, thông qua thông điệp SIP REGISTER.

5. Sau đó:

- Alice gửi một thông điệp ACK đến Redirect Server, rồi
- Gửi lại thông điệp INVITE trực tiếp đến Bob tại domain 2.

6. Bob trả lời bằng một thông điệp ACK gửi lại Alice.

7. Cuối cùng, Alice gửi một ACK đến Bob khi nhận được phản hồi 200 OK từ Bob (xác nhận thiết lập thành công kết nối).

3.3.4.3 Đặc điểm nổi bật của giải pháp

- **Mã hóa đầu cuối:** Mỗi gói thoại được mã hóa bằng khóa phiên riêng biệt
- **Cấu trúc phân lớp:** Giải pháp tách rời dữ liệu thoại, điều khiển và bảo mật → giúp xử lý nhanh hơn
- **Tạo khóa động:** Sử dụng thuật toán sinh khóa nhẹ để giảm tải tính toán
- **Chính sách động:** Cho phép thay đổi thuật toán và độ mạnh mã hóa tùy theo chất lượng mạng hiện tại
- **Tương thích thời gian thực:** Kiến trúc đảm bảo xử lý đủ nhanh để hỗ trợ thoại không độ trễ

3.3.4.4 Ưu điểm so với VPN truyền thống

Tiêu chí	VPN truyền thống	Giải pháp đề xuất
Mã hóa	Cứng nhắc	Linh hoạt theo chính sách
Xử lý dữ liệu thoại	Không tối ưu	Tối ưu hóa theo luồng thoại
Tải tính toán	Cao	Thấp
QoS	Không đảm bảo	Có hỗ trợ
Hỗ trợ thời gian thực	Kém	Tốt

Bảng 3. Bảng so sánh ưu điểm với VPN truyền thống

3.4 Khắc phục các lỗ hổng bảo mật trong triển khai mạng không dây dựa trên VPN

Các khuyến nghị thực tiễn tốt nhất hiện nay cho triển khai mạng không dây doanh nghiệp thường đề xuất sử dụng VPN từ phía máy khách không dây nhằm đảm bảo xác thực và quyền riêng tư. Một vấn đề bảo mật nghiêm trọng với mô hình triển khai như vậy, gọi là lỗ hổng "bộ định tuyến không dây ẩn" (Hidden Wireless Router – HWR).

Lỗ hổng này vốn có trong kiến trúc mạng LAN không dây sử dụng VPN, khiến các máy khách vô tình trở thành kênh truyền cho các cuộc tấn công, khai thác các tính năng phổ biến hiện có trong hệ điều hành như Windows và Linux.

3.4.1 Giới thiệu

Với sự phổ biến của card mạng không dây 802.11 và laptop tích hợp chip Wi-Fi, nhu cầu truy cập không dây phổ quát đang trở thành hiện thực. Tuy nhiên, bảo mật là vấn đề then chốt trong việc triển khai mạng không dây cho doanh nghiệp.

Truy cập không dây trực tiếp vào mạng nội bộ doanh nghiệp có thể làm mất hiệu lực của các công cụ bảo mật như firewall và hệ thống phát hiện xâm nhập (IDS), vốn được triển khai để bảo vệ khỏi mối đe dọa từ Internet.

Ngoài ra, môi trường mạng không dây là một môi trường mở, dễ bị truy cập bởi bất kỳ ai ở gần vật lý (trong vùng phủ sóng radio) của mạng doanh nghiệp.

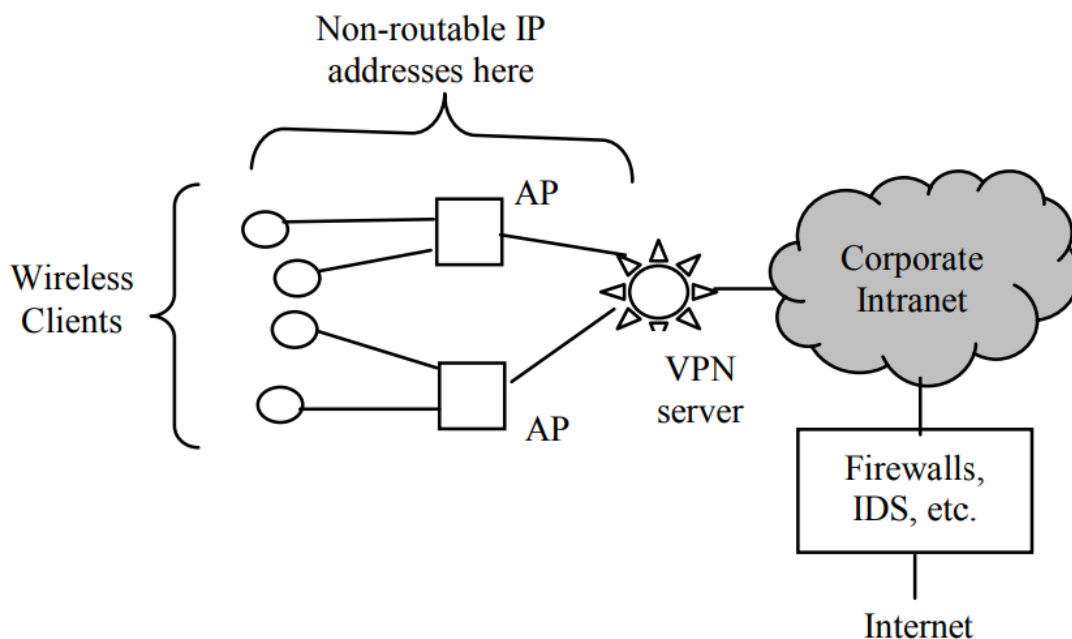
Triển khai ban đầu của mạng 802.11 sử dụng WEP (Wired Equivalent Privacy) để bảo mật truyền thông. Tuy nhiên, hiện nay đã rõ rằng WEP có những hạn chế nghiêm trọng và không đủ an toàn.

Đáp lại nhu cầu bảo mật mạnh hơn, nhóm làm việc IEEE 802.11 đã thành lập Task Group i nhằm phát triển phiên bản bảo mật nâng cao cho tiêu chuẩn 802.11, dẫn đến chuẩn 802.11i.

Chuẩn mới 802.11i được xây dựng dựa trên xác thực theo cổng 802.1X cho người dùng và thiết bị, nhằm khắc phục hầu hết các vấn đề bảo mật của WEP. Đặc biệt, 802.11i cung cấp:

- Xác thực theo người dùng
- Khóa mạnh theo phiên (mã hóa)
- Và các tính năng bảo mật nâng cao khác

802.11i đã trải qua nhiều lần sửa đổi để vá các lỗ hổng bảo mật đã biết. Dự kiến các thiết bị hỗ trợ chuẩn 802.11i sẽ sớm xuất hiện trên thị trường. Tuy nhiên, sẽ mất một thời gian nữa trước khi 802.11i được triển khai rộng rãi.



Hình 45 Chiến lược triển khai mạng không dây hiện tại

Trong lúc chờ đợi 802.11i được triển khai rộng rãi, nhiều doanh nghiệp đã sử dụng kiến trúc dựa trên VPN như là “phương pháp tốt nhất” để bảo mật mạng không dây của họ.

Như thể hiện trong Hình 45, mạng không dây và mạng có dây được phân tách bằng một máy chủ VPN.

Các máy khách được cấu hình để sử dụng WEP nhằm kết nối tới các Access Point (AP). Tuy nhiên, WEP không được xem là cung cấp mức bảo mật đáng tin cậy.

Sau khi kết nối thành công, máy khách nhận một địa chỉ IP không định tuyến được (non-routable), ví dụ như 192.168.1.32 thông qua DHCP. Tiếp theo:

- Máy khách khởi tạo kết nối VPN tới máy chủ VPN (ví dụ: 192.168.1.1)
- Phần mềm VPN client trên máy người dùng thường là cùng một client được dùng để truy cập từ xa vào mạng doanh nghiệp (ví dụ từ nhà)
- Sau khi thực hiện xác thực và trao đổi khóa, một kênh bảo mật (tunnel) được thiết lập để truyền thông và truy cập Intranet nội bộ doanh nghiệp.
- Kết nối VPN yêu cầu xác thực theo người dùng. Rõ ràng, với kiến trúc này, tất cả các lợi ích của VPN (bảo mật, riêng tư, xác thực...) đều đạt được.
- Đặc biệt, các gói dữ liệu trên sóng vô tuyến được mã hóa, và cung cấp mức độ riêng tư tương đương với IPsec.

Kiến trúc VPN dựa trên mô hình này được lựa chọn bởi vì:

- Đơn giản, dễ triển khai
- Có thể triển khai bằng phần mềm và phần cứng sẵn có
- Đội ngũ IT doanh nghiệp đã quen thuộc với công nghệ VPN (IPSec hoặc PPTP)
- Hầu hết các laptop hiện nay đã cài sẵn client IPSec để truy cập từ xa

3.4.2 Bộ định tuyến không dây ẩn (*Hidden Wireless Router – HWR*)

Hầu hết các thiết bị không dây, đặc biệt là laptop tích hợp kết nối không dây, đều được trang bị hai card mạng (dual-NICs), ví dụ:

- Một card không dây tích hợp chuẩn 802.11
 - Một card mạng có dây (Ethernet)
- Nhiều doanh nghiệp cung cấp cả:
- Cổng Ethernet vật lý
 - Và mạng Wi-Fi dùng VPN bảo mật (theo kiến trúc ở hình trên)
 - Nhằm tạo điều kiện cho người dùng kết nối mạng nội bộ từ bất kỳ vị trí nào trong tòa nhà.

Người dùng có thể:

- Cắm dây vào jack Ethernet
- Kết nối với mạng Wi-Fi qua VPN
- Hoặc dùng cả hai giao diện cùng lúc

Thông thường, các jack Ethernet này là “mở”, tức không yêu cầu xác thực — mặc dù trong một số trường hợp có thể kích hoạt xác thực theo chuẩn 802.1X.

3.4.2.1 Lỗ hổng tiềm tàng từ cấu hình hệ điều hành

Kiến trúc hiện tại ngầm giả định rằng người dùng sẽ không sử dụng cả hai giao diện mạng (wired và wireless) cùng lúc, và sẽ không cấu hình thiết bị để làm bộ định tuyến. Nhưng giả định này có thể bị phá vỡ một cách dễ dàng, do:

- Các tính năng chia sẻ kết nối (Internet Connection Sharing)
- Cấu hình NAT/bridging có sẵn trong hệ điều hành như Windows và Linux
- Người dùng có thể chủ ý hoặc vô tình bật tính năng này, hoặc thậm chí bị phần mềm độc hại (Trojan) cấu hình thiết bị theo cách đó

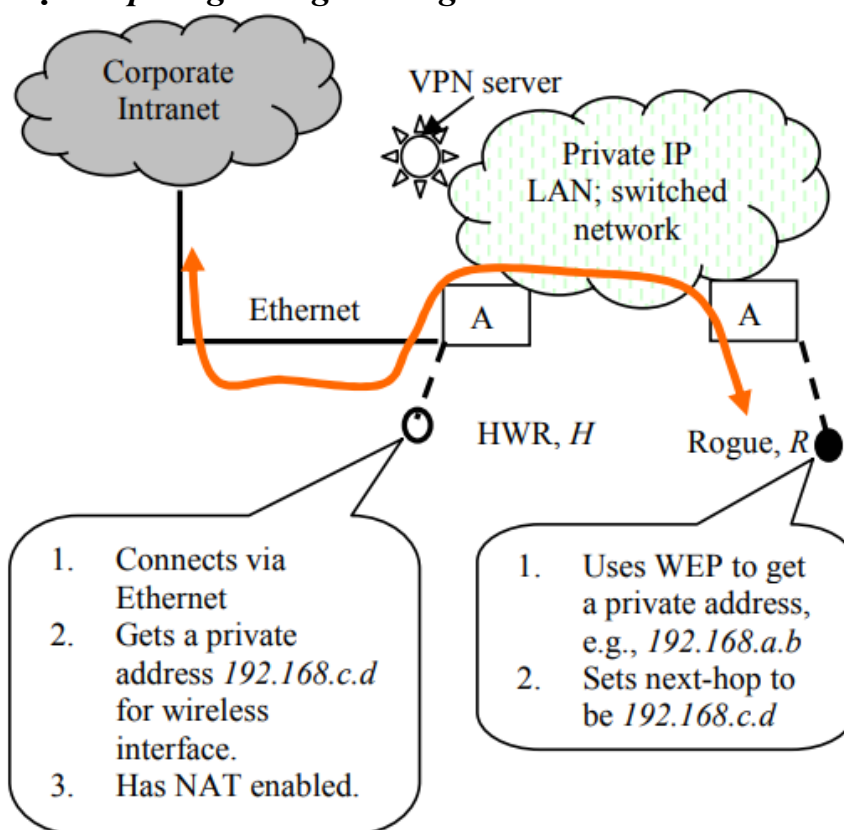
Và từ đó, thiết bị của người dùng trở thành một “bộ định tuyến không dây ẩn (HWR)”, mở ra đường đi trực tiếp cho các thiết bị không xác thực xâm nhập vào mạng doanh nghiệp – mà không cần đi qua VPN server.

3.4.2.2 Hậu quả thực tế

Lỗ hổng HWR cho phép thực hiện:

- Wardriving: quét Wi-Fi từ xe hơi ngoài bãi đậu xe
- Kịch bản "xâm nhập từ bãi đậu xe" – attacker kết nối đến HWR thông qua sóng Wi-Fi
- Tấn công từ các sảnh chờ, hành lang, tầng không được bảo vệ trong công ty
 - Bản chất lỗ hổng này làm suy yếu toàn bộ cơ chế VPN, bởi attacker không cần xác thực qua VPN mà vẫn truy cập được vào mạng nội bộ thông qua HWR.

3.4.3 Phát hiện và phòng chống lỗ hổng HWR



Hình 46 Mô tả chi tiết tình huống tấn công

Trong mô hình bảo mật hiện tại, các máy khách không dây đều được thiết kế để chỉ có thể truy cập mạng nội bộ thông qua VPN server. Để làm điều này, hệ thống chỉ cấp cho các máy kết nối với Access Point một địa chỉ IP không định tuyến được (non-routable), ví dụ như 192.168.x.x.

Tuy nhiên, vấn đề phát sinh từ một giả định sai lầm: đó là người dùng sẽ không bật chia sẻ kết nối hoặc NAT.

3.4.3.1 Kịch bản minh họa (xem Hình 46 trên):

- Một laptop có hai card mạng (có dây và không dây), được gọi là **máy H**:

- Giao diện không dây được kết nối với AP và có IP nội bộ (private)
- Giao diện có dây kết nối đến mạng nội bộ (Intranet) qua Ethernet, nhận địa chỉ IP định tuyến được
- Gói tin từ máy H gửi tới intranet sẽ đi trực tiếp qua giao diện có dây, không qua VPN server.

Giả sử người dùng đã bật NAT hoặc chia sẻ kết nối (Internet Connection Sharing) trên laptop H. Nếu một thiết bị rogue (máy R) gửi các gói dữ liệu đến máy H:

- Các gói tin (và cả phản hồi từ mạng) sẽ được chuyển tiếp thông qua H, đi vào mạng nội bộ
- Không đi qua VPN, không bị kiểm soát bởi tường lửa hoặc xác thực
- Kết quả: máy R đã đột nhập vào mạng doanh nghiệp, chỉ cần:
- Có thể kết nối tới cùng AP (dù chỉ cần WEP yếu)
- Không cần tài khoản VPN hoặc bất kỳ xác thực nào
- Chính vì thế, gọi đây là lỗ hổng Hidden Wireless Router – HWR: Máy hợp pháp H đang vô tình hoạt động như một router không dây ẩn, dù người dùng có biết hay không.

3.4.3.2 Mức độ nghiêm trọng

HWR không phụ thuộc vào việc có bật xác thực 802.1X trên cổng Ethernet hay không, vì:

- Gói tin đã được gửi **từ trong nội bộ** qua NAT
- Máy H là thiết bị nội bộ được cấp quyền hợp lệ

Ngoài ra, việc cấu hình một laptop hai card mạng để làm NAT router rất dễ dàng:

- Trên Windows:
 - Dễ dàng bật Internet Connection Sharing (ICS)
 - Chọn “chia sẻ kết nối có dây” ra giao diện không dây
 - Windows sẽ tự động gán địa chỉ 192.168.0.1 cho giao diện không dây
 - Sau đó, giao diện không dây vẫn có thể được cấu hình lại để nhận IP qua DHCP → hoàn tất việc chia sẻ mạng

Ngay cả khi không cấu hình DHCP, miễn là máy rogue và máy H cùng kết nối đến một AP, thì rogue vẫn có thể sử dụng H làm cổng chuyển tiếp.

3.4.3.3 Giải pháp phát hiện HWR – dựa trên sniffing và cấu hình AP

Một thiết bị tấn công rogue client R có thể giả lập địa chỉ IP thuộc cùng subnet với địa chỉ IP riêng của HWR H (ví dụ: 192.168.0.5), và gửi các gói tin qua H như thể nó là gateway mặc định. Những gói này sẽ không đi qua VPN Server, và thay vào đó được chuyển tiếp thẳng vào mạng nội bộ doanh nghiệp – một điều hoàn toàn trái với mong đợi của kiến trúc mạng hiện tại.

Các Access Point và switch thường hoạt động như thiết bị chuyển mạch tầng 2, vì vậy các gói từ máy R có thể dễ dàng được chuyển tiếp đến máy H.

Quan sát thấy rằng cấu hình như vậy hoàn toàn có thể xảy ra theo nhiều cách:

- Máy tính bị nhiễm virus hoặc worm trong mạng công cộng (public network)
- Người dùng vô tình cấu hình sai do chuyển đổi qua lại giữa môi trường công ty và gia đình
- Phần mềm tự động bật chia sẻ mạng mà người dùng không hề hay biết

Điều khiến cho vấn đề HWR trở nên đặc biệt nguy hiểm là khả năng kích hoạt rất dễ dàng – thậm chí không cần sự hiểu biết hoặc đồng thuận của người dùng.

Một số điểm quan sát từ lỗ hổng HWR:

- Thứ nhất, khi chỉ quan sát việc kết nối AP và hoạt động DHCP, không thể phát hiện được điều bất thường nào giữa R và H. Trong thực tế, các card không dây tích hợp trong laptop thường tự động kết nối và lấy địa chỉ IP – điều này là hành vi hoàn toàn "hợp lệ".
- Thứ hai, R và H không cần phải nằm trong phạm vi sóng Wi-Fi trực tiếp với nhau. Gói tin từ R vẫn có thể được chuyển tiếp qua mạng LAN có dây (corporate switched network) và đến được H thông qua các Access Point đã kết nối trước đó. Điều này chứng minh rằng HWR là một lỗ hổng nguy hiểm hơn cả “Rogue Access Point”, vốn yêu cầu phải cắm thiết bị AP giả mạo vào jack Ethernet nội bộ.
- Thứ ba, ví dụ được trình bày trong ngữ cảnh laptop có hai giao diện mạng (có dây và không dây). Tuy nhiên, lỗ hổng này vẫn tồn tại ngay cả với các laptop chỉ có kết nối không dây, nếu như:
 - VPN client không được sử dụng
 - Hoặc VPN client **cho phép chia sẻ kết nối** (như Microsoft PPTP client)

Ví dụ, nếu bật chia sẻ kết nối Internet (ICS) trên giao diện logic PPTP VPN của Windows, các gói từ mạng không VPN cũng có thể đi qua, dẫn đến vi phạm toàn bộ mô hình bảo mật.

Giải pháp dựa trên giám sát (Monitoring-Based Solutions)

Đây là giải pháp dựa trên việc giám sát lưu lượng trong mạng không dây. Các thiết bị thực hiện giám sát này được gọi là

Sniffer có thể:

- Nghe thụ động các gói tin trên không gian vô tuyến
- Hoặc cũng có thể là các trạm (station) được kết nối vào mạng không dây để theo dõi luồng lưu lượng

1. Phát hiện HWR

Trong kịch bản HWR, an ninh bị xâm phạm vì một thiết bị không xác thực VPN có thể truy cập vào mạng nội bộ doanh nghiệp bằng cách vượt qua máy chủ VPN.

Nói cách khác: Kết nối không dây bảo vệ bằng VPN chỉ “an toàn” khi tất cả lưu lượng buộc phải đi qua VPN server.

Do đó, để phát hiện một thiết bị đang hoạt động như HWR, cần kiểm tra:

- Các gói tin được gửi bởi máy khách không xác thực VPN mà lại đi đến địa chỉ IP nằm trong mạng nội bộ
- Đặc biệt là khi gói tin đến một máy chủ nội bộ hoặc gửi phản hồi ping từ mạng ngoài VPN

Giải pháp giám sát cần xác định các bất thường sau:

- MAC Address trùng khớp xuất hiện ở cả giao diện không dây và có dây
- IP Source không đúng subnet
- Sử dụng dải địa chỉ không hợp lệ
 - Nếu các điều kiện trên xảy ra, có thể kết luận: một máy đang hoạt động như một router ẩn (HWR).

2. Phát hiện lưu lượng "giao tiếp chéo" (Cross-Traffic Detection)

Trong mô hình mạng được bảo vệ bởi VPN, toàn bộ lưu lượng từ mạng không dây nên được chuyển tới VPN server. Điều này có nghĩa rằng lưu lượng từ các máy trạm không xác thực nên bị chặn.

Do đó, việc theo dõi lưu lượng "giao tiếp chéo" – tức là lưu lượng từ một trạm không dây tới một trạm không dây khác mà không đi qua VPN server – là chìa khóa để phát hiện HWR.

Giao tiếp chéo có thể dễ dàng được nhận diện bởi các thiết bị sniffer chỉ cần quan sát tiêu đề MAC của các khung 802.11, thay vì toàn bộ gói tin.

Bằng cách theo dõi lưu lượng và trao đổi thông tin giữa các sniffer, hệ thống có thể:

- Xây dựng danh sách các địa chỉ MAC của các trạm không dây và AP đang kết nối
- Xác định lưu lượng giao tiếp chéo: tức các khung có địa chỉ nguồn và đích đều là các trạm không dây

Ngoài ra, sniffer cũng có thể được cấu hình trước với danh sách địa chỉ MAC được phép làm đích, ví dụ:

- Địa chỉ của máy chủ VPN
- Hoặc gateway của VPN
 - Từ đó, sniffer có thể phát hiện các gói không hướng đến đích được phép, và ngăn cản các hoạt động đáng ngờ.

Dù sniffer không có khóa WEP, nó vẫn có thể phát hiện lưu lượng bất thường, bởi vì:

- Phần header của khung 802.11 không bị mã hóa
- Các tiêu đề MAC vẫn truyền "rõ ràng" qua không trung

Tuy nhiên, nếu có thể giải mã WEP, sniffer sẽ có thể:

- Xây dựng bản đồ tương ứng giữa địa chỉ MAC và IP trong các khung đã quan sát
- Nếu một địa chỉ MAC xuất hiện với nhiều địa chỉ IP, điều đó chỉ ra khả năng đang có một router hoạt động
- Nếu địa chỉ MAC đó thuộc về một trạm không dây → rất có thể đó là một HWR

3. Phát hiện HWR theo cách chủ động

Các phương pháp mô tả trước đó chủ yếu mang tính thụ động. Tuy nhiên, HWR cũng có thể bị phát hiện theo cách chủ động, vì khác với các kịch bản NAT truyền thống trong mạng có dây, chúng ta có quyền truy cập vào phía bên kia của NAT – cụ thể là giao diện không dây.

- Điều này cho phép thiết bị giám sát (sniffer) gửi gói tin trực tiếp tới HWR qua giao diện không dây, và quan sát xem có nhận được phản hồi hay không.

Cách thực hiện:

- Sniffer (thiết bị giám sát) tham gia mạng Wi-Fi với tư cách là một trạm.

- Nó sẽ cố gắng thiết lập kết nối đến một “honeypot” – máy chủ môi trong mạng có dây, thông qua HWR làm gateway.
- Nói cách khác, sniffer đóng vai trò như một máy client rogue.

Nếu máy chủ môi nhận được gói tin và phản hồi lại:

- Khi sniffer nhận được phản hồi, thiết bị đóng vai trò gateway chính là một HWR.

Thậm chí, honeypot có thể trả về địa chỉ IP nguồn của gói tin nhận được → từ đó, xác định được địa chỉ IP của giao diện có dây trên HWR.

Những mục tiêu bị sniffer dò quét có thể bao gồm:

- Tất cả các máy trạm đang hoạt động
- Hoặc chỉ những trạm đã bị đánh dấu là nghi ngờ thông qua các kỹ thuật phát hiện trước đó

Hạn chế:

- Phương pháp dò quét này không phát hiện được HWR hoạt động với địa chỉ IP ngoài dải địa chỉ private đang được kiểm tra.

4. Định vị và kiểm soát HWR sau khi phát hiện

Sau khi xác định được một HWR tiềm năng, cần thực hiện các bước:

- Xác định vị trí vật lý của HWR
- Ngăn chặn việc nó tiếp tục hoạt động như một router

Cách định vị:

- Nếu dùng phương pháp giám sát thụ động:
 - Có thể ước lượng vị trí HWR dựa vào cường độ tín hiệu sóng không dây (RSSI)
 - Nếu dùng phương pháp dò quét chủ động:
 - Có thể truy vết từ địa chỉ IP của giao diện có dây của HWR
 - Dựa vào bản đồ switch – port – số hiệu jack mạng
 - Có thể dùng IP đó để truy vết người dùng tương ứng từ cơ sở dữ liệu
- Nhờ vậy, hệ thống có thể hiện cảnh báo trên máy tính HWR, hoặc gửi cảnh báo tới người dùng liên quan.

Ngăn chặn tạm thời:

Tuy nhiên, việc tìm người dùng, thông báo và xử lý từ phía máy khách có thể tốn thời gian.

- Trong khi chờ xử lý, HWR cần được vô hiệu hóa ngay lập tức bằng các phương pháp không phụ thuộc vào máy khách, ví dụ:
- Ngắt kết nối Wi-Fi (vô hiệu MAC từ phía AP)
- Vô hiệu hóa cổng mạng vật lý dựa trên IP của giao diện có dây

Giải pháp dựa trên Access Point (AP-based Solutions)

Trong khi các giải pháp dựa trên giám sát (monitor-based) cung cấp khả năng phát hiện và xử lý sau khi HWR đã hoạt động, thì các giải pháp dựa trên Access Point (AP) hướng tới ngăn chặn việc HWR có thể hoạt động ngay từ đầu.

Nguyên lý chính

Nếu khả thi, Access Point có thể chặn kịch bản HWR bằng cách lọc frame (khung dữ liệu) dựa trên:

- Địa chỉ MAC nguồn và đích, và
 - Địa chỉ IP được sử dụng trong các gói tin
- Cụ thể, AP có thể được cấu hình để:
- Không cho phép lưu lượng giữa các máy trạm không dây (peer-to-peer)
 - Chỉ cho phép lưu lượng đến và đi từ một số đích cụ thể, ví dụ: VPN server chính và dự phòng

Lo ngại về khả năng quản lý

Một phản biện phổ biến với phương pháp kiểm soát truy cập dựa trên AP là:

- Khó quản lý
- Không mở rộng tốt (không scalable)

Tuy nhiên, giải pháp được đề xuất trong tài liệu này không gặp phải hạn chế đó, vì:

- Danh sách địa chỉ cho phép (access list) được giới hạn chỉ vài mục, ví dụ:
 - VPN Server chính
 - VPN Server dự phòng
- Danh sách chỉ cần cập nhật khi cấu hình VPN server thay đổi
 - Do đó, phương pháp kiểm soát dựa trên AP là khả thi, đơn giản, hiệu quả và dễ duy trì.

Từ cả hai phía mạng

- Từ phía không dây (wireless):

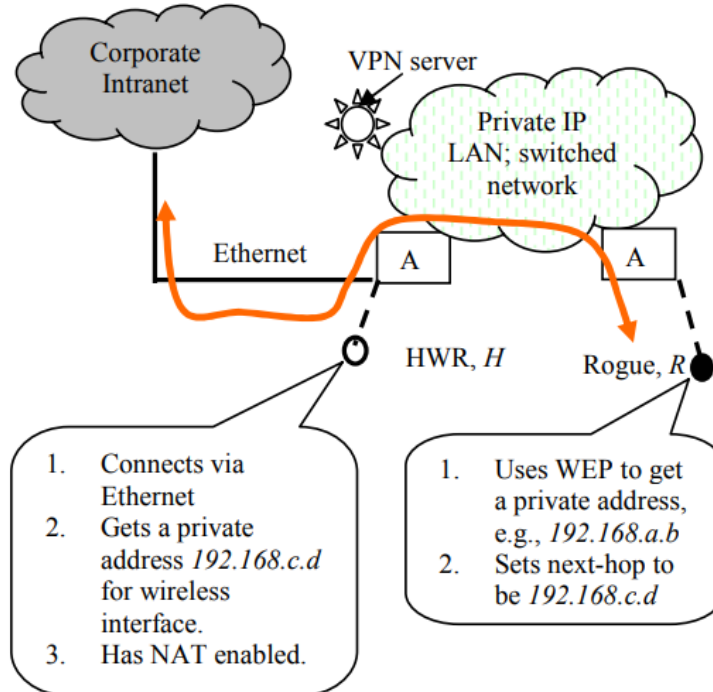
- AP có thể sử dụng tính năng kiểm soát truy cập theo MAC (MAC-based Access Control)
- Nếu một thiết bị được phát hiện là HWR, AP có thể thêm địa chỉ MAC của nó vào danh sách cấm
- Gửi disassociate message để buộc ngắt kết nối
- Từ phía có dây (wired):
 - Cổng mạng mà HWR kết nối vào có thể bị vô hiệu hóa
 - Switch hoặc router có thể được cấu hình để chặn lưu lượng đến từ thiết bị đó
- Lưu ý: Việc phát hiện và kiểm soát HWR cũng có liên quan đến các vấn đề an ninh mạng không dây khác như:
- Giả mạo địa chỉ MAC/IP
- Tấn công từ chối dịch vụ (DoS)

3.5 Kết chương

Chương 3 phân tích sâu các lỗ hổng bảo mật có thể xảy ra khi triển khai VPN và đưa ra những giải pháp thực tế như IDS kết hợp khai phá dữ liệu, mô hình liên nhà cung cấp (Inter-Provider VPN), và tấn công vào HWR. Qua đó, chương giúp tăng cường nhận thức về an toàn thông tin khi xây dựng mạng riêng ảo.

CHƯƠNG 4. DEMO SỬ DỤNG GIẢI PHÁP DỰA TRÊN GIÁM SÁT (MONITORING-BASED SOLUTIONS) ĐỂ PHÁT HIỆN LỖ HỔNG HWR

4.1 Chuẩn bị mô hình mạng



- H (Windows 10) – Máy hợp pháp, có 2 NIC (làm HWR)
- R (Kali Linux) – Rogue attacker
- S (Kali Linux) – Sniffer giám sát Wi-Fi
- VPN Server (Windows Server 2019/2022) – Mô phỏng mạng nội bộ có bảo vệ VPN

Sử dụng VMnet8 làm NIC1 và Vmnet12 làm NIC2:

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.106.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.197.0
VMnet11	Host-only	-	Connected	-	192.168.100.0
VMnet12	Host-only	-	Connected	-	10.10.19.0

Hình 47 Cấu hình mạng máy ảo

4.2 CẤU HÌNH CHUNG CHO CÁC MÁY ẢO

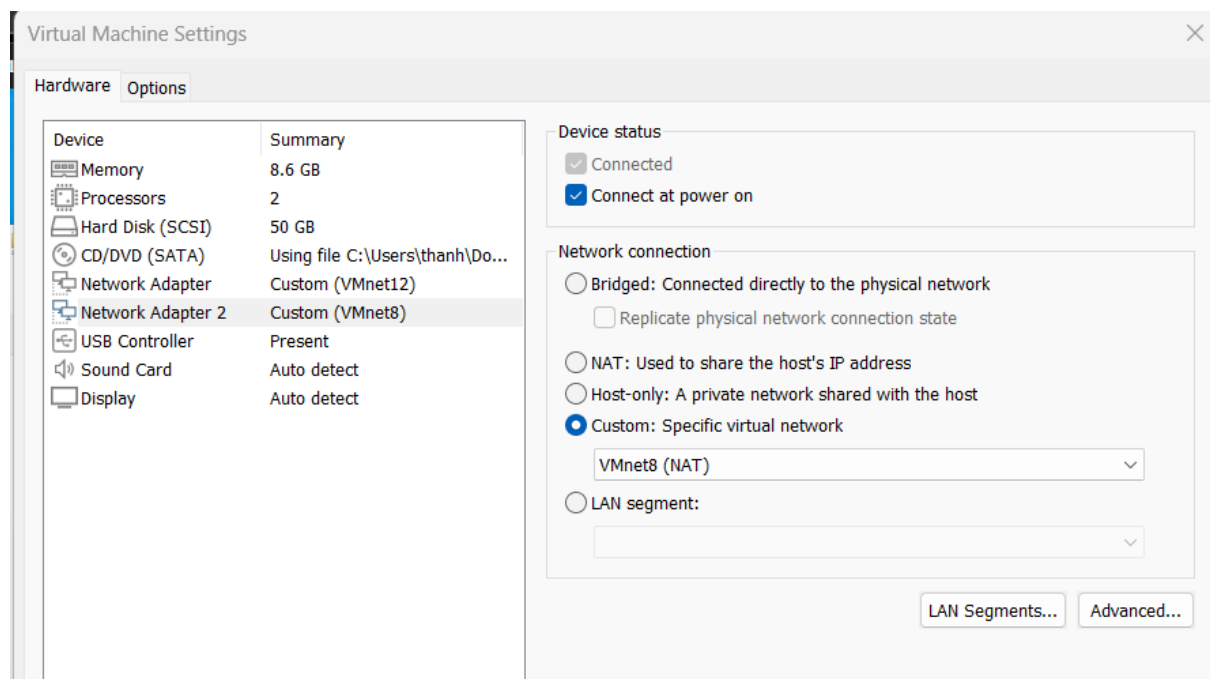
Thành phần	Cấu hình đề xuất
RAM	2–4 GB cho mỗi máy (H/S/R), 4–8 GB cho VPN Server
CPU	2 Core trở lên
Disk	30–50 GB /máy
Vmware Version	VMware Workstation 16.x hoặc VMware Player 17.x trở lên
Mạng VMware	Tạo sẵn 2 loại adapter: "NAT" và "Host-only"

Bảng 4. Bảng cấu hình thành phần các máy ảo

4.2.1 Máy H (Windows 10 - HWR)

Cấu hình:

- Ethernet (VMnet12) – chính là NIC2 (nối VPN server)
- Ethernet 2 (VMnet8) – là NIC1 (WiFi nội bộ, nối tới máy R, S)



Hình 48 Cấu hình 2 NIC máy H

- Cài đặt địa chỉ ip, 2 dải địa chỉ là : 192.168.197.129 và 10.10.19.10

```

Unknown adapter VPN - VPN Client:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . : fe80::d810:cfd1:8a94:9833%4
IPv4 Address. . . . . : 192.168.197.129
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.197.2

Ethernet adapter Ethernet1:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . : fe80::ecb4:726f:a45b:9a21%7
IPv4 Address. . . . . : 10.10.19.10
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . :

```

Hình 49 Cấu hình IP máy H

- Sau đó bật Internet Connection Sharing (ICS) trên NIC2 để chia sẻ sang NIC1.

4.2.2 Máy R (Kali Linux - Attacker)

Cấu hình:

- NIC: VMnet8 (NAT)
- Cài IP tĩnh cho VMnet8 (cùng dải):

```
sudo ip addr add 192.168.197.100/24 dev eth0
```

```
sudo ip route add default via 192.168.197.129
```

```

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:62:44:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.197.100/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe62:4497/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$

```

Hình 50 Cấu hình IP máy r

4.2.3 Máy S (Kali Linux - Sniffer)

Cấu hình:

- NIC: VMnet8 (NAT)

- Cài IP cho VMnet8 (cùng dải), địa chỉ IP máy S là: 192.168.197.149

```
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ef:4e:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.197.149/24 brd 192.168.197.255 scope global dynamic noprefixroute eth0
        valid_lft 1778sec preferred_lft 1553sec
    inet6 fe80::c8a3:96fd:c2b3:17f/64 scope link
```

Hình 51 Cấu hình IP máy S

4.2.4 Máy VPN Server (Windows Server)

Cấu hình:

- NIC: VMnet12 (Host-only)
- Cài đặt địa chỉ IP tĩnh: 10.10.19.5

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b77b:16ab:8ec4:1e0d%14
    IPv4 Address. . . . . : 10.10.19.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\Administrator>
```

Hình 52 Cấu hình IP máy VPN Server

4.2.5 Kiểm tra cấu hình

- Từ máy H ping đến máy VPN Server

```
C:\Windows\system32>ping 10.10.19.5

Pinging 10.10.19.5 with 32 bytes of data:
Reply from 10.10.19.5: bytes=32 time=19ms TTL=128
Reply from 10.10.19.5: bytes=32 time=2ms TTL=128
Reply from 10.10.19.5: bytes=32 time=2ms TTL=128

Ping statistics for 10.10.19.5:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 19ms, Average = 7ms
```

Hình 53 Từ máy H ping đến máy VPN Server

- Từ máy H ping đến máy R

```
C:\Windows\system32>ping 192.168.197.100

Pinging 192.168.197.100 with 32 bytes of data:
Reply from 192.168.197.100: bytes=32 time=13ms TTL=64
Reply from 192.168.197.100: bytes=32 time=7ms TTL=64

Ping statistics for 192.168.197.100:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 13ms, Average = 10ms
```

Hình 54 Từ máy H ping đến máy R

- Từ máy H ping đến máy Sniffer

```
C:\Windows\system32>ping 192.168.197.149

Pinging 192.168.197.149 with 32 bytes of data:
Reply from 192.168.197.129: Destination host unreachable.
Reply from 192.168.197.129: Destination host unreachable.

Ping statistics for 192.168.197.149:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Control-C
^C
C:\Windows\system32>
```

Hình 55 Từ máy H ping đến máy Sniffer

- Từ máy R ping đến máy H qua dải 192.169.197.129

```
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ ping 192.168.197.129
PING 192.168.197.129 (192.168.197.129) 56(84) bytes of data.
64 bytes from 192.168.197.129: icmp_seq=1 ttl=128 time=2.96 ms
64 bytes from 192.168.197.129: icmp_seq=2 ttl=128 time=1.42 ms
^C
— 192.168.197.129 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.418/2.191/2.964/0.773 ms

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ █
```

Hình 56 Từ máy R ping đến máy H

- Từ máy R ping đến máy Sniffer

```
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ ping 192.168.197.149
PING 192.168.197.149 (192.168.197.149) 56(84) bytes of data.
64 bytes from 192.168.197.149: icmp_seq=1 ttl=64 time=6.26 ms
64 bytes from 192.168.197.149: icmp_seq=2 ttl=64 time=4.15 ms
64 bytes from 192.168.197.149: icmp_seq=3 ttl=64 time=1.88 ms
^C
R — 192.168.197.149 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 1.875/4.096/6.262/1.791 ms

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
```

Hình 57 Từ máy R ping đến máy Sniffer

- Từ máy Sniffer ping đến máy H

```
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ ping 192.168.197.129
PING 192.168.197.129 (192.168.197.129) 56(84) bytes of data.
64 bytes from 192.168.197.129: icmp_seq=1 ttl=128 time=1.05 ms
64 bytes from 192.168.197.129: icmp_seq=2 ttl=128 time=0.535 ms
64 bytes from 192.168.197.129: icmp_seq=3 ttl=128 time=3.36 ms
^C
— 192.168.197.129 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.535/1.649/3.361/1.228 ms
```

Hình 58 Từ máy Sniffer ping đến máy H

- Từ máy sniffer ping đến máy R

```
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ ping 192.168.197.100
PING 192.168.197.100 (192.168.197.100) 56(84) bytes of data.
64 bytes from 192.168.197.100: icmp_seq=1 ttl=64 time=191 ms
64 bytes from 192.168.197.100: icmp_seq=2 ttl=64 time=5.00 ms
64 bytes from 192.168.197.100: icmp_seq=3 ttl=64 time=4.58 ms
^C
— 192.168.197.100 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 4.581/66.986/191.381/87.960 ms
```

Hình 59 Từ máy Sniffer ping đến máy R

4.3 CÁC BƯỚC THỰC HIỆN

4.3.1 Trên máy Sniffer

4.3.1.1 Xác định lại interface mạng:

- Ghi nhớ tên interface đang có IP dải 192.168.197.x (ví dụ: eth0, eth1, ens33, ...)

✓ Ở đây là eth0

4.3.1.2 Chạy tcpdump để bắt gói

- Lệnh bắt toàn bộ gói từ máy Rogue → mạng nội bộ:

sudo tcpdump -i eth0 dst net 10.10.19.0/24

```
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ sudo tcpdump -i eth0 dst net 10.10.19.0/24
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Hình 60 Lệnh bắt toàn bộ gói

4.3.2 Từ máy R (Kali – Rogue), thực hiện gửi gói không qua VPN ping 10.10.19.5

```
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ ping 10.10.19.5
PING 10.10.19.5 (10.10.19.5) 56(84) bytes of data.
64 bytes from 10.10.19.5: icmp_seq=1 ttl=127 time=8.53 ms
64 bytes from 10.10.19.5: icmp_seq=2 ttl=127 time=6.93 ms
64 bytes from 10.10.19.5: icmp_seq=3 ttl=127 time=5.31 ms
64 bytes from 10.10.19.5: icmp_seq=4 ttl=127 time=5.61 ms
^C
— 10.10.19.5 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 5.310/6.594/8.526/1.271 ms
```

Hình 61 Ping từ máy R đến máy VPN Server

curl http://10.10.19.5

```
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ curl http://10.10.19.5
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
}

#container {
    margin-left:auto;
    margin-right:auto;
    text-align:center;
}

a img {
    border:none;
}
-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clid=0x409"></a>
</div>
</body>
</html>
```

Hình 62 Máy R truy cập địa chỉ máy VPN Server

4.3.3 Quan sát từ Sniffer

- Thấy gói tin từ 192.168.197.x → 10.10.19.x xuất hiện trên tcpdump
 - ✓ Đã phát hiện truy cập bất thường → chứng minh lỗ hổng HWR có tồn tại


```
(kali@b22dcatt253-DinhThiThanhTam)~$ sudo tcpdump -i eth0 dst net 10.10.19.0/24
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
05:20:46.203609 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 45065, seq 1, length 64
05:20:47.205771 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 45065, seq 2, length 64
05:20:48.206074 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 45065, seq 3, length 64
05:20:49.207809 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 45065, seq 4, length 64
05:20:52.411454 IP 192.168.197.100.52674 > 10.10.19.5.http: Flags [S], seq 1727339503, win 64240, options [mss 1460,sackOK,TS val 2880325600 ecr 0,nop,wscale 7], length 0
05:20:52.414720 IP 192.168.197.100.52674 > 10.10.19.5.http: Flags [P], seq 0:74, ack 1, win 502, length 74: HTTP: GET / HTTP/1.1
05:20:52.414721 IP 192.168.197.100.52674 > 10.10.19.5.http: Flags [P], seq 0:74, ack 1, win 502, length 74: HTTP: GET / HTTP/1.1
05:20:52.421910 IP 192.168.197.100.52674 > 10.10.19.5.http: Flags [F], seq 74, ack 929, win 495, length 0
05:20:52.421917 IP 192.168.197.100.52674 > 10.10.19.5.http: Flags [F], seq 74, ack 929, win 495, length 0
05:20:52.426426 IP 192.168.197.100.52674 > 10.10.19.5.http: Flags [F], seq 74, ack 929, win 495, length 0
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Hình 63 Quan sát từ máy Sniffer

4.3.4 Kết quả phân tích gói tin:

Gói ICMP (ping):

IP 192.168.197.100 > 10.10.19.5: ICMP echo request

- Cho thấy máy R (192.168.197.100) đã gửi gói ping đến máy VPN Server (10.10.19.5)
- Đã thoát ra khỏi mạng 192.168.197.0/24 và đi về phía 10.10.19.0/24
- Nghĩa là ICS trên máy H đang hoạt động tốt (đã NAT & forward)

Gói HTTP:

IP 192.168.197.100.52674 > 10.10.19.5.http: Flags [P], seq ..., HTTP: GET / HTTP/1.1

IP 10.10.19.5.http > 192.168.197.100.52674: Flags [F], ack ...

Cho thấy máy VPN server đã phản hồi lại gói HTTP. Điều này chứng minh rằng:

- Đã có kết nối 2 chiều thành công giữa máy R ↔ máy VPN Server
- NAT ICS trên máy H đang hoạt động đúng
- Máy R hoàn toàn có thể thực hiện sniffing/tấn công HWR

4.3.5 Có thể lọc chi tiết hơn

- Lọc theo IP nguồn (máy Rogue):

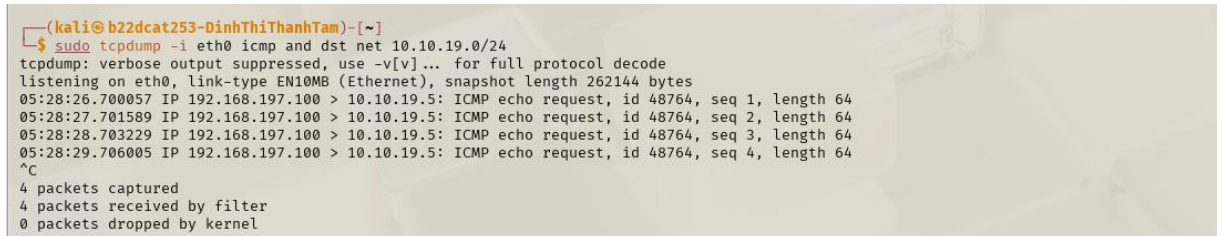
sudo tcpdump -i eth0 src 192.168.197.100 and dst net 10.10.19.0/24

```
(kali@b22dcatt253-DinhThiThanhTam)~$ sudo tcpdump -i eth0 src 192.168.197.100 and dst net 10.10.19.0/24
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
05:27:27.954403 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 48286, seq 1, length 64
05:27:28.956372 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 48286, seq 2, length 64
05:27:29.955533 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 48286, seq 3, length 64
05:27:30.957668 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 48286, seq 4, length 64
05:27:33.214338 IP 192.168.197.100.53140 > 10.10.19.5.http: Flags [S], seq 284594517, win 64240, options [mss 1460,sackOK,TS val 2880726403 ecr 0,nop,wscale 7], length 0
05:27:33.222795 IP 192.168.197.100.53140 > 10.10.19.5.http: Flags [P], seq 0:74, ack 1, win 502, length 74: HTTP: GET / HTTP/1.1
05:27:33.226366 IP 192.168.197.100.53140 > 10.10.19.5.http: Flags [P], seq 0:74, ack 1, win 502, length 74: HTTP: GET / HTTP/1.1
05:27:33.231139 IP 192.168.197.100.53140 > 10.10.19.5.http: Flags [F], seq 74, ack 929, win 495, length 0
05:27:33.233143 IP 192.168.197.100.53140 > 10.10.19.5.http: Flags [F], seq 74, ack 929, win 495, length 0
05:27:33.242735 IP 192.168.197.100.53140 > 10.10.19.5.http: Flags [F], seq 74, ack 929, win 495, length 0
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Hình 64 Lọc theo IP nguồn

- Lọc ICMP (ping):

sudo tcpdump -i eth0 icmp and dst net 10.10.19.0/24



```
(kali@b22dcat253-DinhThiThanhTam)~  
$ sudo tcpdump -i eth0 icmp and dst net 10.10.19.0/24  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
05:28:26.700057 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 48764, seq 1, length 64  
05:28:27.701589 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 48764, seq 2, length 64  
05:28:28.703229 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 48764, seq 3, length 64  
05:28:29.706005 IP 192.168.197.100 > 10.10.19.5: ICMP echo request, id 48764, seq 4, length 64  
^C  
4 packets captured  
4 packets received by filter  
0 packets dropped by kernel
```

Hình 65 Lọc ICMP (ping)

- ✓ Kết luận: chứng minh R đã truy cập nội bộ.

4.4 Kết chương

Chương này đã trình bày quá trình mô phỏng và kiểm thử giải pháp giám sát lưu lượng mạng để phát hiện lỗ hổng HWR (Host with Wireless Router). Thông qua mô hình gồm các máy H (ICS), R (attacker), S (sniffer) và VPN Server, ta đã chứng minh:

Máy R có thể truy cập trái phép vào mạng nội bộ thông qua máy H bật ICS.

Sniffer bắt được các gói ICMP và HTTP gửi từ R đến VPN Server.

ICS trên H hoạt động như một gateway, tạo điều kiện cho tấn công vượt VPN.

Kết quả cho thấy, lỗ hổng HWR là có thật, và giám sát lưu lượng là một phương pháp hiệu quả để phát hiện. Tuy nhiên, để đảm bảo an toàn, cần bổ sung các biện pháp như kiểm soát ICS, dùng NAC, hoặc triển khai IDS/IPS trong mạng.

KẾT LUẬN

Qua quá trình nghiên cứu và thực hành, báo cáo đã cung cấp cái nhìn toàn diện về công nghệ **VPN (Virtual Private Network)**, từ các khái niệm cơ bản, cấu trúc hệ thống, phân loại giao thức đến các vấn đề bảo mật đi kèm. Đặc biệt, phần thực nghiệm mô phỏng tấn công HWR đã cho thấy tính thực tiễn của việc triển khai và giám sát VPN trong các mô hình mạng hiện đại.

Kết quả phân tích cho thấy rằng, bên cạnh những ưu điểm nổi bật như bảo mật dữ liệu, mã hóa kết nối và ẩn danh truy cập, VPN vẫn tồn tại một số rủi ro tiềm ẩn nếu không được triển khai và quản lý đúng cách. Các lỗ hổng như chia sẻ kết nối (ICS), cấu hình sai, hoặc thiếu cơ chế giám sát có thể bị tin tặc khai thác để vượt qua lớp bảo mật VPN và xâm nhập vào mạng nội bộ.

Việc xây dựng mô hình thực nghiệm và sử dụng giải pháp giám sát (monitoring-based) để phát hiện hành vi truy cập trái phép từ thiết bị Rogue đã chứng minh được hiệu quả của các biện pháp giám sát mạng trong phòng chống tấn công HWR. Điều này không chỉ củng cố kiến thức lý thuyết mà còn nâng cao kỹ năng thực hành và tư duy phản biện về an toàn mạng cho sinh viên.

Trong tương lai, để nâng cao hơn nữa khả năng bảo vệ VPN, cần kết hợp nhiều giải pháp như xác thực đa yếu tố (MFA), phân đoạn mạng (network segmentation), kiểm soát truy cập (NAC), và triển khai hệ thống IDS/IPS. Như vậy, việc bảo vệ hệ thống VPN sẽ đạt được hiệu quả toàn diện hơn trước các mối đe dọa ngày càng tinh vi trong môi trường mạng hiện đại.

TÀI LIỆU THAM KHẢO

- [1] Google Cloud (2023). “Cloud VPN Architecture and Security.”
- [2] IEEE Xplore (2021). “VPN-as-a-Service: Design and Implementation.”
- [3] Cisco (2023). “SD-WAN and VPN Integration for Enterprise Networks.”
- [4] Cloudflare (2024). “Post-Quantum Cryptography in VPNaaS: Challenges and Solutions.”
- [5] <https://media.techtarget.com/searchNetworking/downloads/Buildvpn1.pdf>
- [6] Mạng riêng ảo VPN là gì? 5 ưu điểm nổi bật của VPN có thể bạn chưa biết, <https://huynhquiiit.com/mang-rieng-ao-vpn-la-gi-5-uu-diem-noi-bat-cua-vpn-co-the-ban-chua-biet/>
- [7] Các mô hình VPN: <https://vnpro.vn/thu-vien/mang-vpn-sitetosite-2358.html>
- [8] William Stallings, *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson Education, 2020.
- [9] NIST Special Publication 800-77, *Guide to IPsec VPNs*, National Institute of Standards and Technology, 2021.
Link: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf>
- [10] Cisco Systems, *VPN Technologies Overview: IPsec, SSL VPN, MPLS VPN*, Cisco White Papers, 2022.
Link: <https://www.cisco.com>
- [11] Đinh Trường Duy, Phạm Hoàng Duy, *Giáo trình An toàn mạng*, Học viện Công nghệ Bưu chính Viễn thông, 2021.
- [12] Nguyễn Hữu Tuấn, *An toàn thông tin và bảo mật mạng*, NXB Bách Khoa Hà Nội, 2020.
- [13] Kali Linux Documentation – *Networking Configuration & Penetration Testing*, Offensive Security, 2022.
Link: <https://www.kali.org/docs/>
- [14] StrongSwan Documentation, *IPsec-based VPN Solution for Linux*, strongSwan Project.
Link: <https://wiki.strongswan.org/>

- [15] RFC 4301 – *Security Architecture for the Internet Protocol*, Internet Engineering Task Force (IETF), 2005.
Link: <https://datatracker.ietf.org/doc/html/rfc4301>
- [16] Phạm Văn Hùng, *Báo cáo nghiên cứu: Phát hiện truy cập trái phép qua ICS trong VPN*, Đại học Bách khoa TP.HCM, 2022.
- [17] *The Design of Secure Embedded VPN Gateway*, Proceedings of the International Conference on Network Security, 2021.
- [18]